FortiADC-VM™ Install Guide — D-Series

Version 4.8.x

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, August 23, 2017

FortiADC-VM Install Guide — D-Series

Revision 4

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-08-23	• Initial release. • Changed "n < 60,000 — 2 GB vRAM; 60, 001 < n < 140, 000 —4 GB vRAM" to "1 < n < 140,000 — 4 GB vRAM". See p. 26. • Changed minimum vRAM from "1 GB" to "2 GB". See p. 26.

Chapter 1: Getting Started

This chapter includes the following information:

Introduction

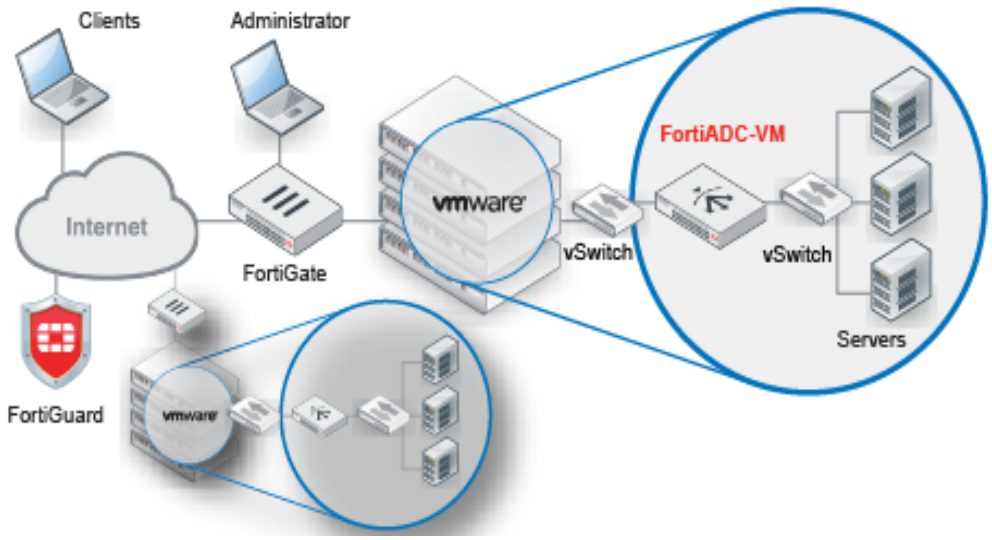
Welcome, and thank you for selecting Fortinet Technologies, Inc. products for your network. The FortiADC D-series family of Application Delivery Controllers (ADC) optimizes the availability, user experience, performance and scalability of enterprise application delivery.

The FortiADC D-series family includes physical appliances and virtual appliances. FortiADC-VM is a virtual appliance version of FortiADC. FortiADC-VM is suitable for small, medium, and large enterprises.

Basic network topology

Figure 1 shows the network topology when the FortiADC-VM is deployment in a virtual machine environment such as VMware vSphere.

Figure 1: FortiADC-VM network topology



FortiADC intercepts incoming client connections and redistributes them to your servers. FortiADC has some firewall capability. However, because it is designed primarily to provide application availability and load balancing, it should be deployed behind a firewall that focuses on security, such as FortiGate.

In deployments that use the FortiADC global server load balancing feature, each hosting location should have its own FortiADC. For example, if you had server clusters located in New York, Shanghai and Bangalore, you deploy three FortiADC appliances: one in New York, one in Shanghai, and one in Bangalore.

Once the virtual appliance is deployed, you can configure FortiADC-VM via its web UI and CLI, from a web browser and terminal emulator on your management computer.

In the initial setup, the following ports are used:

- DNS lookup — UDP 53
- FortiGuard licensing — TCP 443

System requirements

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5

For best performance, install FortiADC-VM on a “bare metal” hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

Hardware-assisted virtualization (VT) must be enabled in the BIOS.

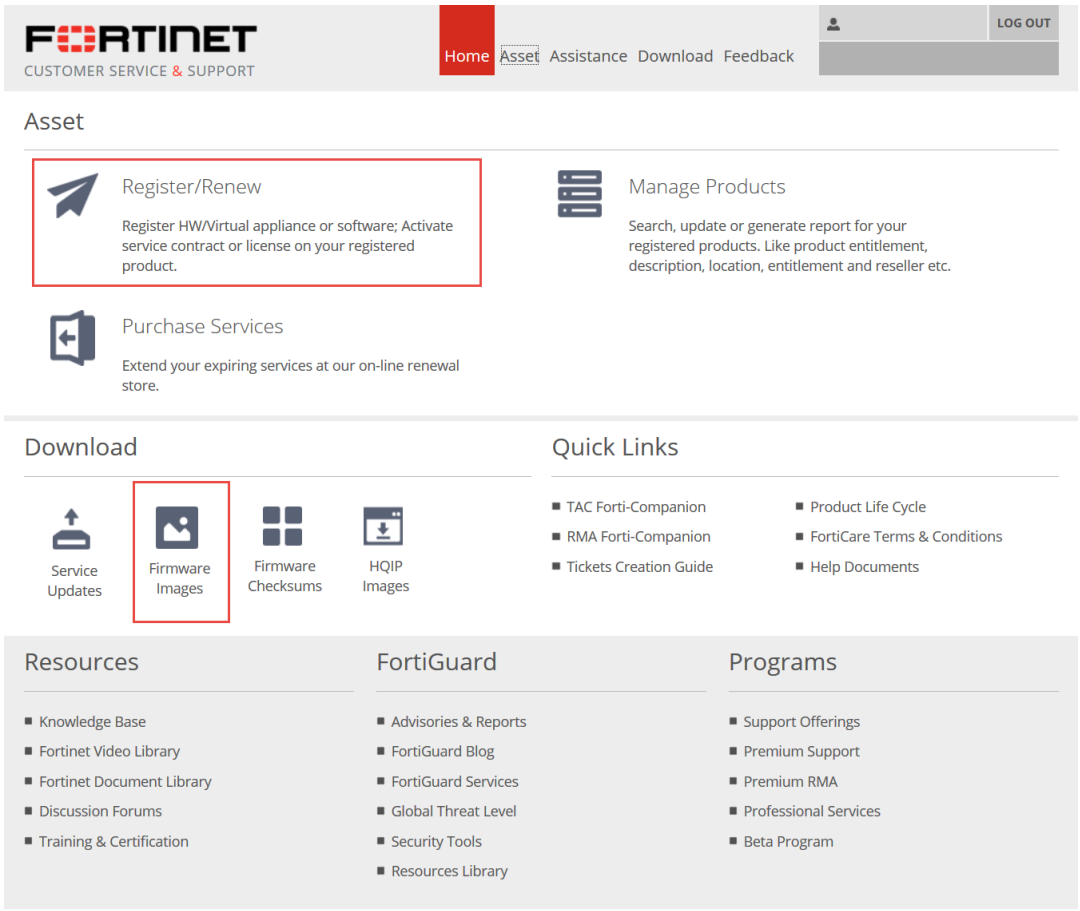
Downloading software & registering with support

When you purchase a FortiADC-VM, you receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase with Fortinet Customer Service & Support so that your FortiADC-VM will be able to validate its license with Fortinet.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration. For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Figure 2 shows the Fortinet Customer Service & Support website.

Figure 2: Fortinet Customer Service & Support



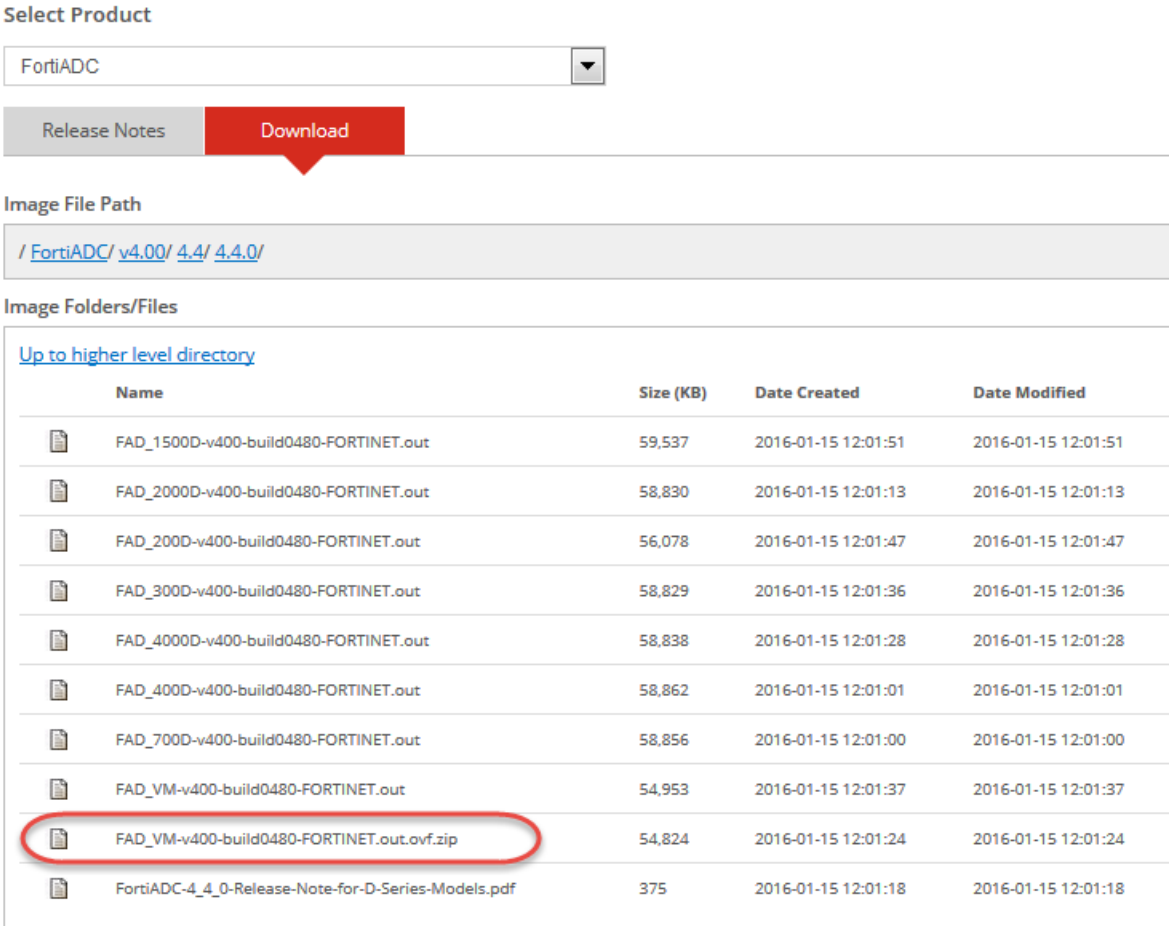
To register & download FortiADC-VM and your license:

1. Log into the Fortinet Customer Service & Support web site:
   https://support.fortinet.com/
2. Under Asset, click **Register/Renew**.
3. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated string of 25 numbers and characters in groups of 5, such as:

   `TLH5R-NUNDP-MC6T7-0DNWA-AP45ZA`

   A registration form appears.
4. Use the form to register your ownership of FortiADC-VM.
   After completing the form, a registration acknowledgment page appears.
5. Click the **License File Download** link.
   Your browser will download the `.lic` file that was purchased for that registration number.
6. Click the **Home** link to return to the initial page.
7. Under Download, click **Firmware Images**.

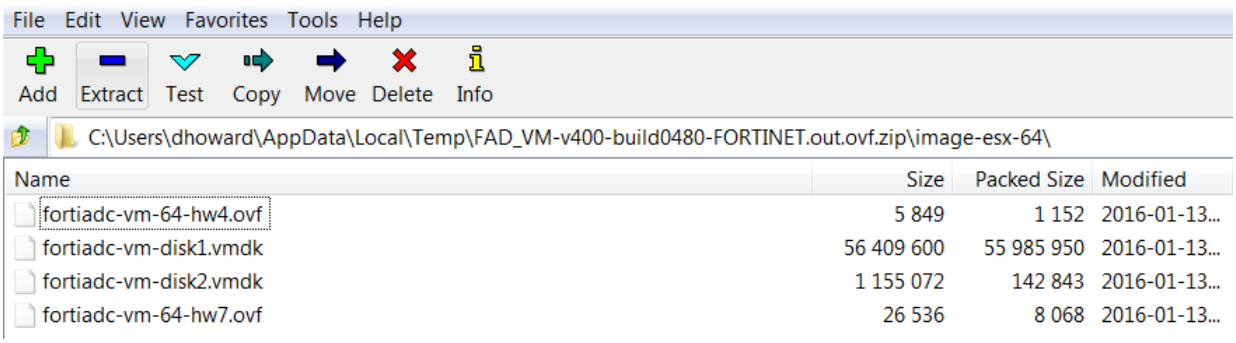
8. Click the FortiADC link and navigate to the version that you want to download.



9. Download the .zip file. You use the VM installation files contained in the .zip file for *new* VM installations. (The `.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)

Files for FortiADC-VM have a `FAD_VM` filename prefix. Other prefixes indicate that the file is for hardware versions of FortiADC such as FortiADC 200D. Such other files cannot be used with FortiADC-VM.

10. Extract the .zip file contents to a folder. The following figure shows the contents of the package for VMware. Refer to the table that follows for details on packages for supported VM environments.



VM environment	Download package
VMware	The ovf.zip download file contains multiple ovf files. The fortiadc-vm-64-hw4.ovf file is a VMware virtual hardware version 4 image that supports ESXi 3.5. The fortiadc-vm-64-hw7.ovf file is a VMware virtual hardware version 7 image that supports ESXi 4.0 and above. Refer to the VMware support site for information about VMware virtual hardware versions and ESXi versions.
Microsoft Hyper-V	The hyperv.zip download file contains multiple files you use for the installation. Extract all the files to a directory you can access when you perform the installation. When you do the installation, you select the folder that contains the unzipped files.
KVM	The kvm.zip download file contains the boot.qcow2 and data.qcow2 files you use for the installation.
Citrix Xen	The xenserver.zip download file contains the fortiadc-vm-xen.ovf file you use for the installation.
Xen Project	The xenopensource.zip download file contains the fortiadc.hvm, bootdisk.img, and logdisk.img files you use for the installation.

Licensing

This section describes licensing. It includes the following information:

- Evaluation license
- License sizes
- License validation

Evaluation license

FortiADC-VM can be evaluated with a free 15-day trial license that includes all features except:

- HA
- FortiGuard updates
- Technical support

You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiADC-VM. When the trial expires, most functionality is disabled. You must purchase a license to continue using FortiADC-VM.

License sizes

FortiADC-VM licenses are available at the following sizing levels.

Table 1: FortiADC-VM sizes

	License/model			
	VM01	VM02	VM04	VM08
Virtual CPUs (vCPUs)	1	2	4	8
Virtual RAM (vRAM)	2 GB	4 GB	8 GB	16 GB

Maximum IP sessions varies by license, but also by available vRAM, just as it does for hardware models. For details, see the maximum configuration values in the *FortiADC Handbook*.

License validation

FortiADC-VM must periodically re-validate its license with the Fortinet Distribution Network (FDN). If it cannot contact the FDN for 24 hours, access to the FortiADC-VM web UI and CLI are locked.

By default, FortiADC-VM attempts to contact FDN over the Internet. If the management port cannot access the Internet (for example, in closed network environments), it is possible for FortiADC-VM to validate its license with a FortiManager that has been deployed on the local network to act as a local FDS (FortiGuard Distribution Server).

On the FortiADC-VM, specify the FortiManager IP address for the "override server" in the FortiGuard configuration:

```
FortiADC-VM # config system fortiguard
   set override-server-status enable
   set override-server-address <fortimanager_ip>:8890
end
```

where <fortimanager_ip> is the IP address. (TCP port 8890 is the port where the built-in FDS feature listens for requests.)

For more information on the FortiManager local FDS feature, see the *FortiManager Administration Guide*.

Note: Although FortiManager can provide FortiGuard security service updates to some Fortinet devices, for FortiADC, its FDN features can provide license validation only.

About this document

This document describes how to deploy a FortiADC virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

This document does *not* cover initial configuration of the virtual appliance itself, nor ongoing use and maintenance. After deploying the virtual appliance, see the *FortiADC Handbook* for information on initial appliance configuration.

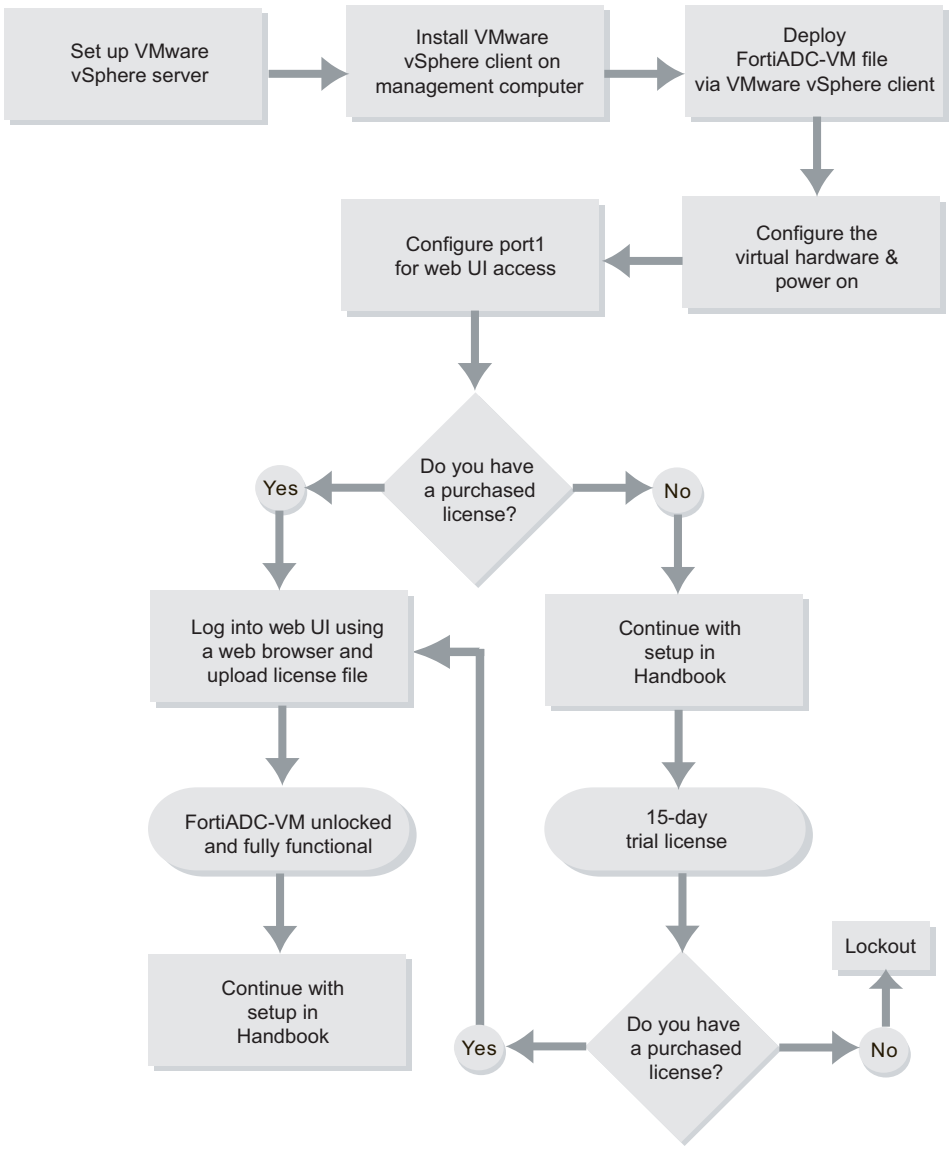
Chapter 2: Deploying FortiADC-VM on VMware vSphere

This chapter provides procedures for deploying FortiADC-VM on VMware vSphere. It includes the following information:

Installation overview

The diagram below gives an overview of the process for installing FortiADC-VM on VMware vSphere, which is described in the subsequent text.

Figure 3: Basic steps for installing FortiADC-VM (VMware)



Step 1: Deploy the OVF file

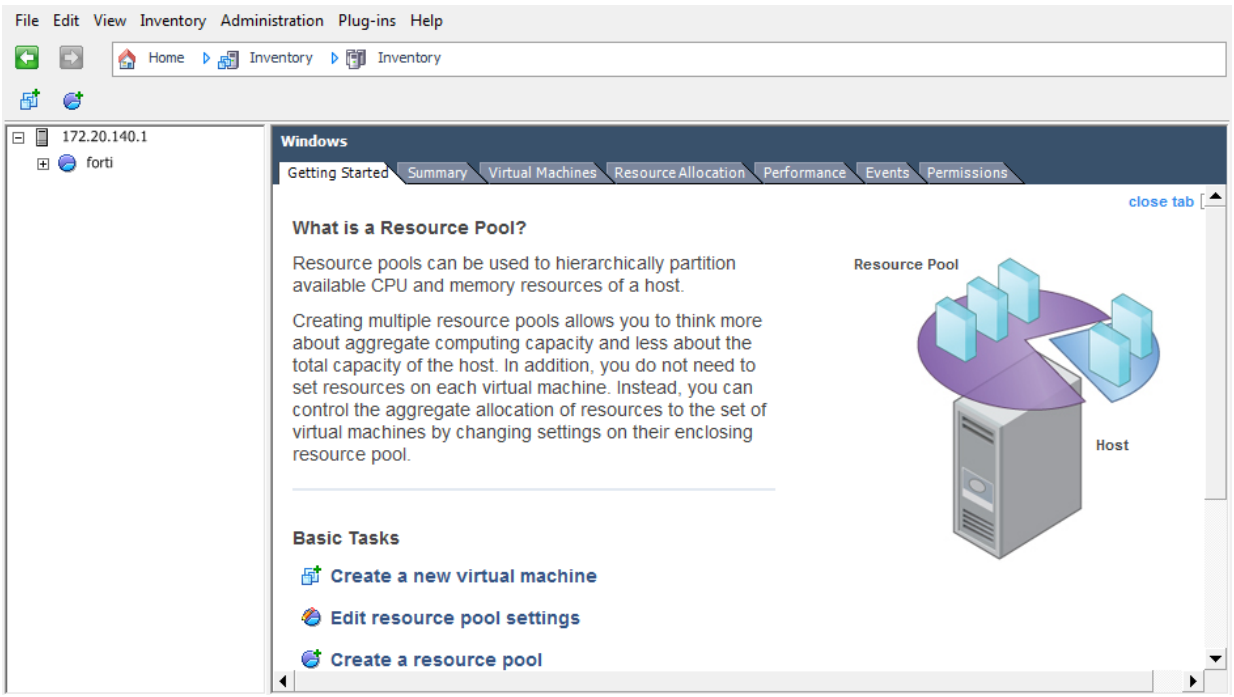
You must first use VMware vSphere Client to deploy the FortiADC-VM OVF package.

To deploy the virtual appliance:

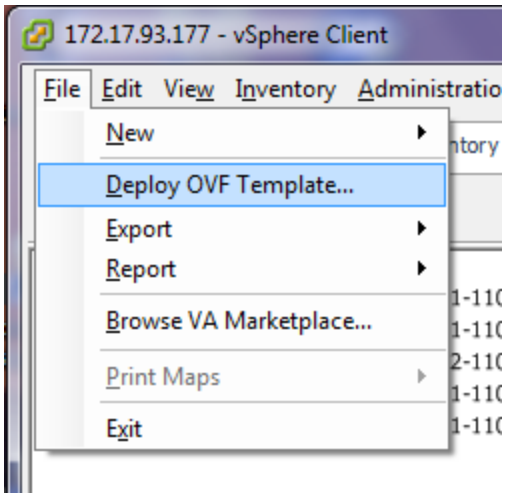
1. Use the VMware vSphere client to connect to VMware vSphere server:
   a. On your management computer, start the VMware vSphere Client.

   b. In IP address / Name, type the IP address or FQDN of the VMware vSphere server.
   c. Enter the username and password, and click **Login**.

   When you successfully log in, the vSphere Client window appears.



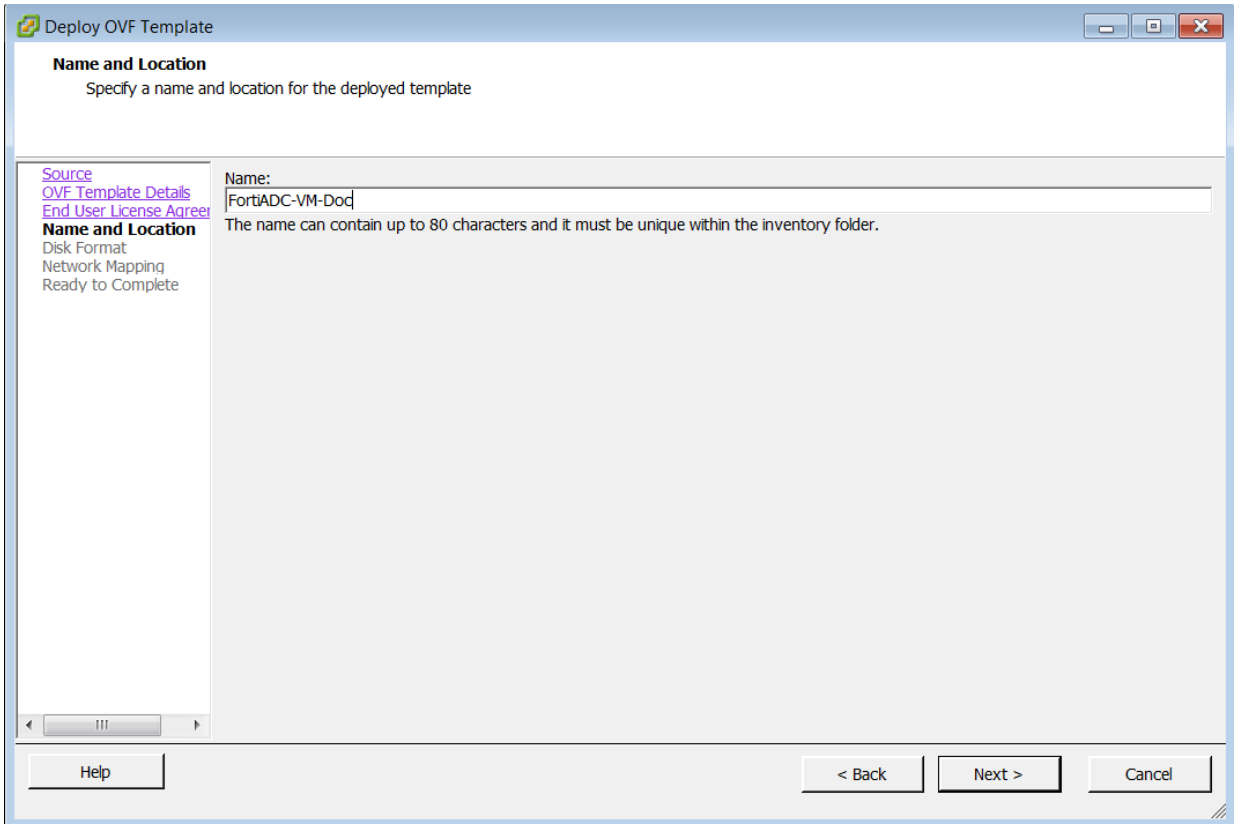
2. Go to File > Deploy OVF Template.



A deployment wizard window appears.

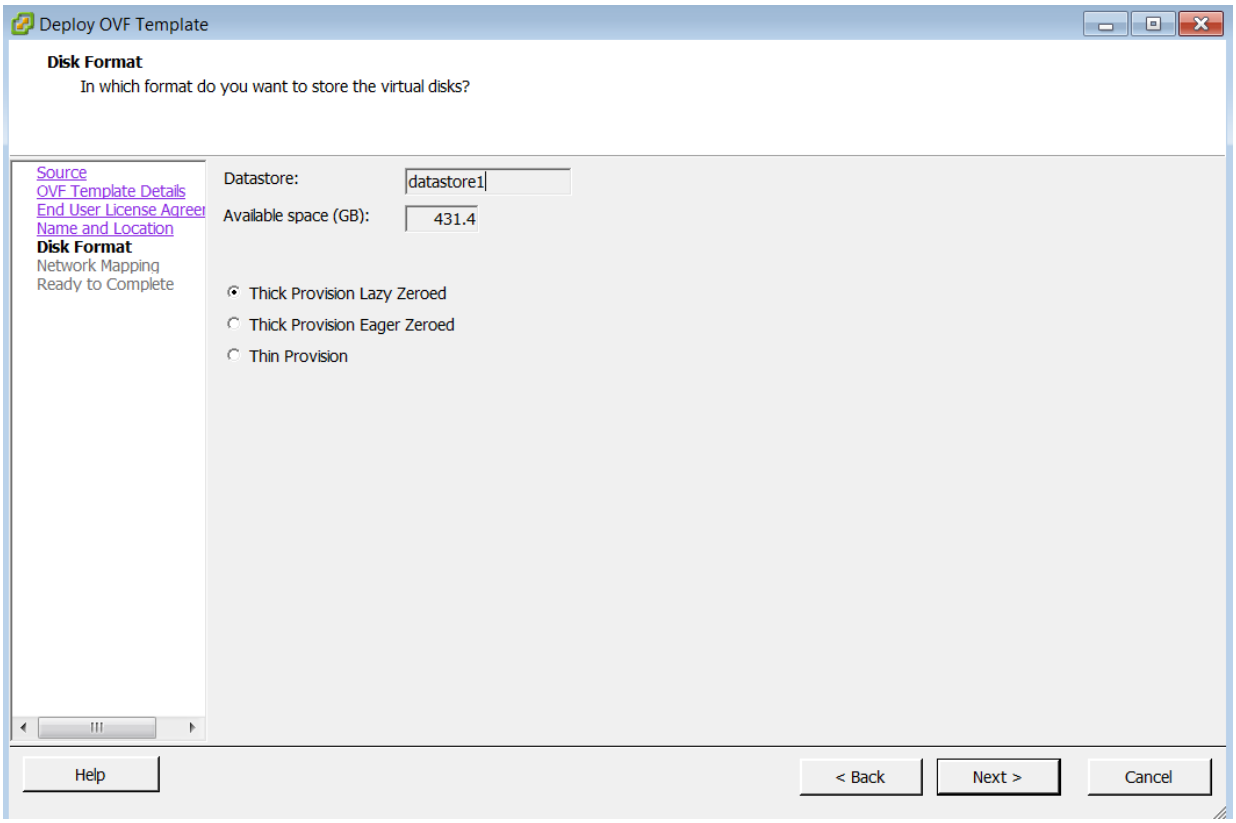
3. In the Deploy OVF Template window, click **Browse** and then locate and select the FortiADC-VM OVF file.
4. Click **Next** twice.
5. On the Name and Location page, type a unique descriptive name for this instance of FortiADC-VM and then then click **Next** to continue.

   The name is the string that appears in the vSphere Client inventory, such as `FortiADC-VM-Doc`. If you plan to deploy multiple instances of this file, consider a naming scheme that makes each VM's purpose or IP address easy to remember. (This name is *not* used as the hostname, nor does it appear within the FortiADC-VM web UI.)

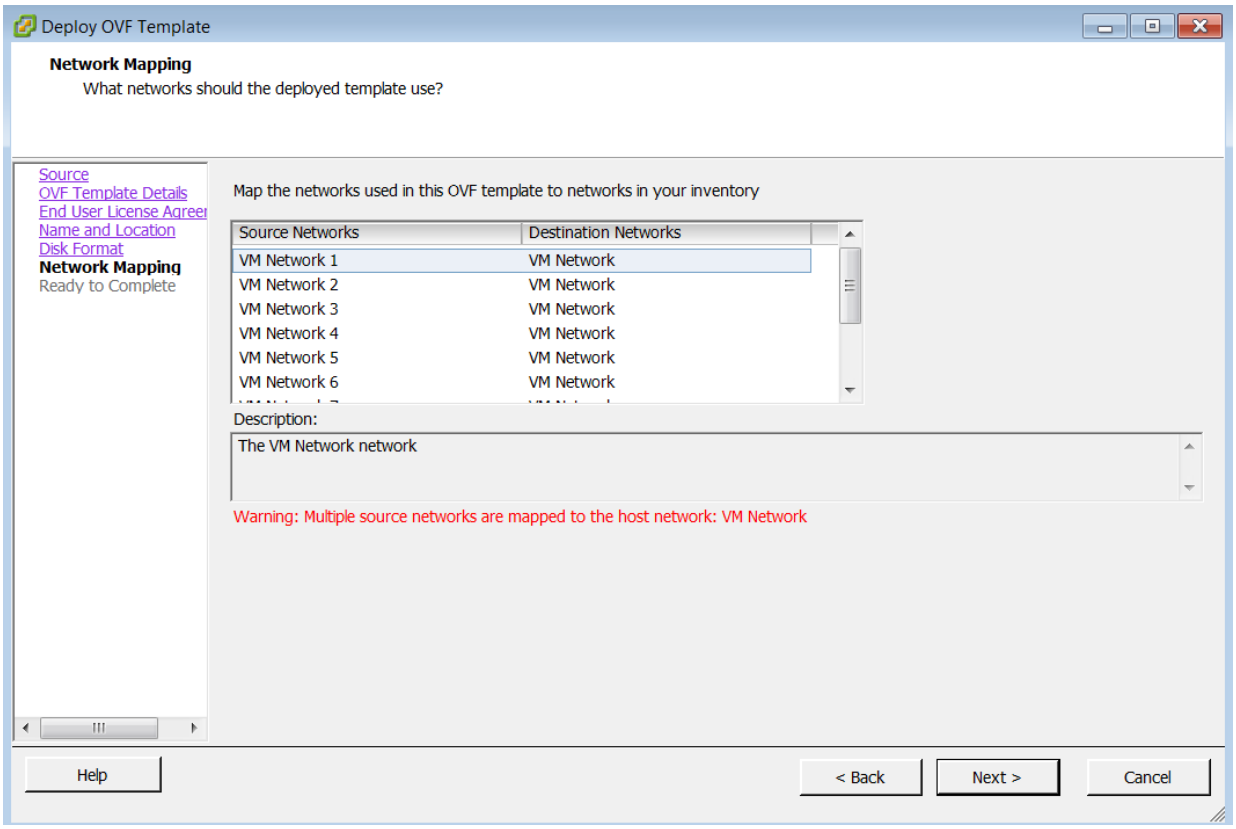


6. On the Disk Format page, select one of the following options and then click **Next** to continue:
   - **Thick provision**— Immediately allocate disk space (specifically 32 GB) for the storage repository.
   - **Thin provision**— Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.

Regardless of your choice here, you must later either allocate or make available at least 40 GB of disk space. 30 GB is only the default minimum value, and is not recommended.



7. On the Network Mapping page, if the hypervisor has more than one possible network mapping for its vSwitch, select the row for the network mapping that FortiADC-VM should use and then then click **Next** to continue.



8. Click **Finish** to close the wizard.

The client connects to the VM environment and deploys the OVF to it. When the operation is complete, the vSphere Client window reappears. The list of virtual machines in the left navigation pane should include your new instance of FortiADC-VM.

Do not power on the virtual appliance until you have completed the following steps:

- Resize the virtual disk (VMDK).
- Set the number of vCPUs.
- Set the vRAM on the virtual appliance.
- Map the virtual network adapter(s).

These settings must be configured in the VM environment, not the FortiADC OS.

Step 2: Configure virtual hardware settings

After deploying the FortiADC-VM image and before powering on the virtual appliance, log into VMware vSphere and configure the virtual appliance hardware settings to suit the size of your deployment.

Table 2 summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Table 2: Virtual hardware settings

Component	Default	Guidelines
Hard disk	32 GB	32 GB is insufficient for most deployments. Upgrade the hard disk before you power on the appliance. After you power on the appliance, you must reformat the FortiADC OS log disk with the following command: `execute formatlogdisk`
CPU	1 CPU	1 CPU is appropriate for a VM01 license. Upgrade to 2, 4, or 8 CPU for VM02, VM04, and VMO8 licenses, respectively.
RAM	2 GB	2 GB is the minimum. See the section on vRAM for guidelines based on expected concurrent connections.
Network interfaces	10 bridging vNICs are mapped to a port group on one virtual switch (vSwitch).	Change the mapping as required for your VM environment and network.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk before powering on the VM appliance.

This step is not applicable if you set up the virtual appliance to use external network file system datastores (such as NFS).

The FortiADC-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. You must resize the vDisk before powering on the virtual machine.

Before doing so, make sure that you understand the effects of the vDisk settings. These options affect the possible size of each vDisk.

1 MB block size — 256 GB maximum file size

2 MB block size — 512 GB maximum file size

4 MB block size — 1024 GB maximum file size

8 MB block size — 2048 GB maximum file size

For example, if you have an 800 GB datastore which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB.

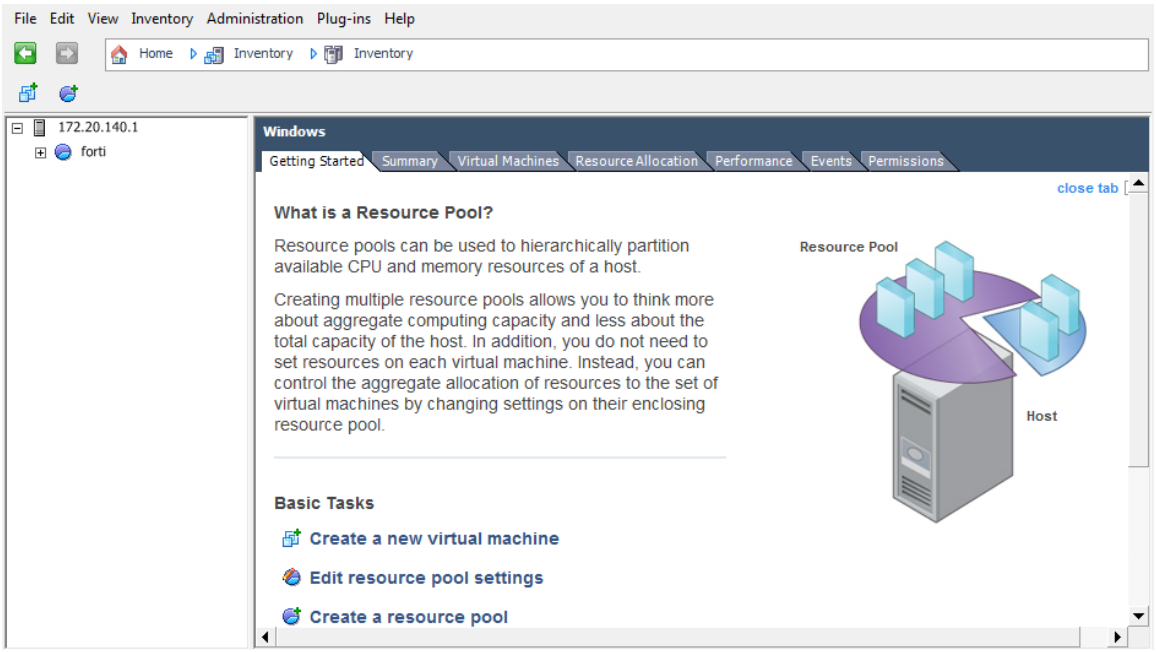
Consider also that, depending on the size of your network, you might require more or less storage for logs, reports, and other data.

For more information on vDisk sizing, see:

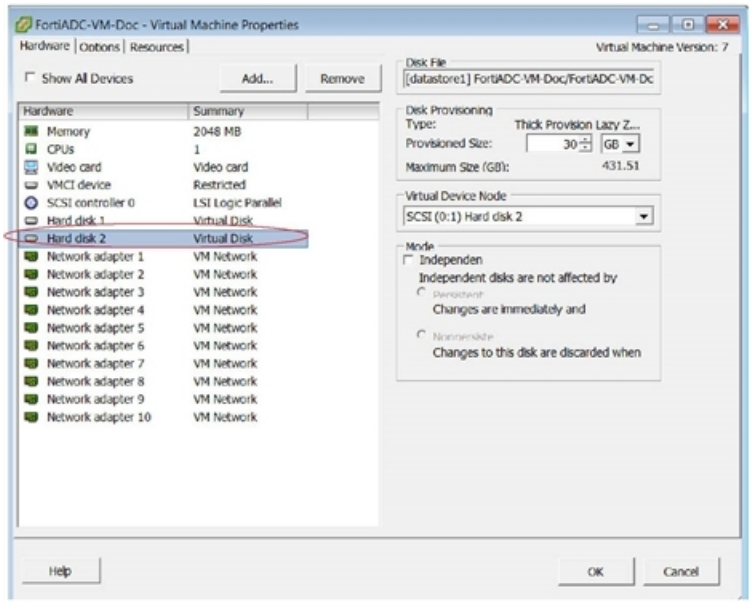
https://communities.vmware.com/docs/DOC-11920

To resize the vDisk:

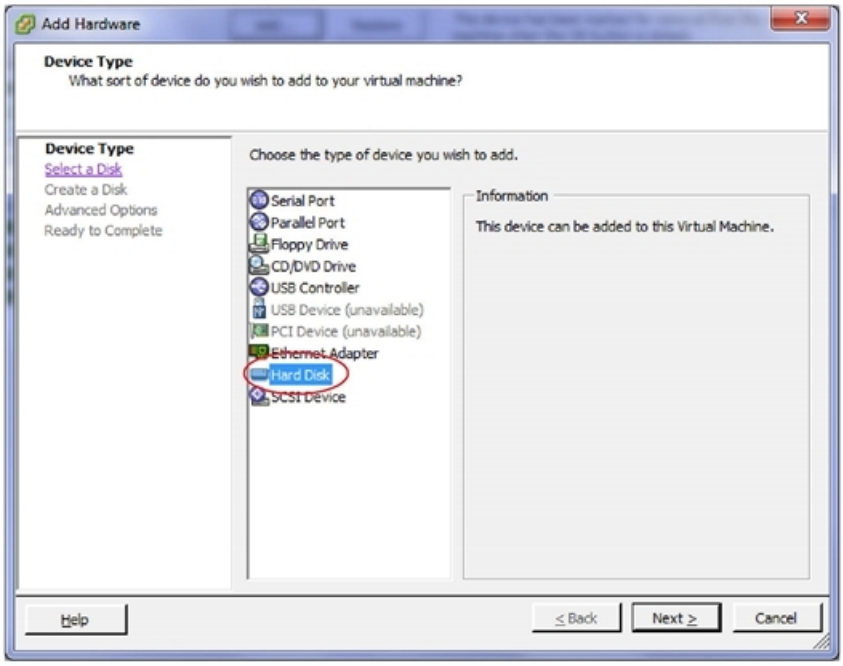
1. Use the VMware vSphere client to connect to VMware vSphere server.
   The following figure shows the vSphere client manager window.



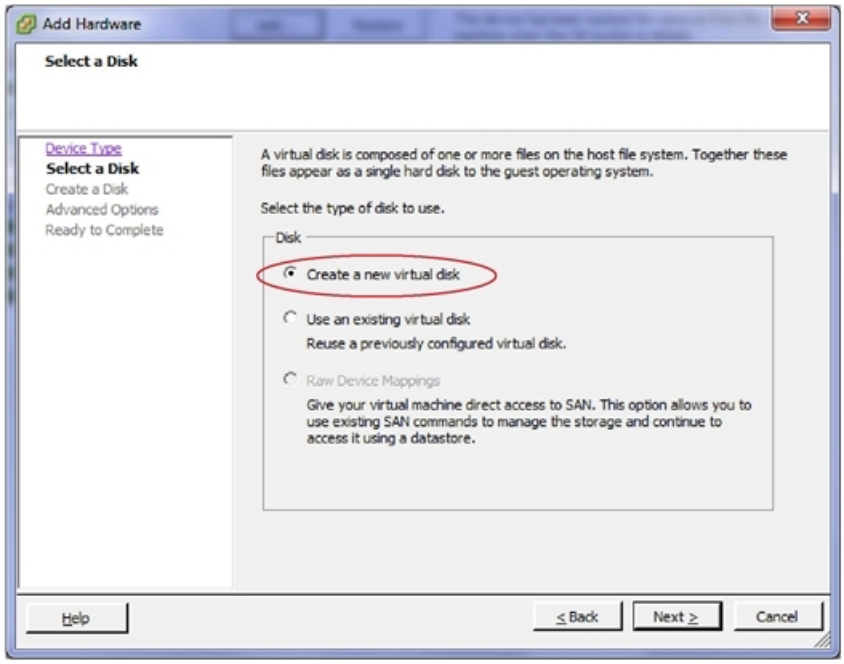
2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, and then select **Edit Settings**.
   The virtual appliance properties dialog appears.



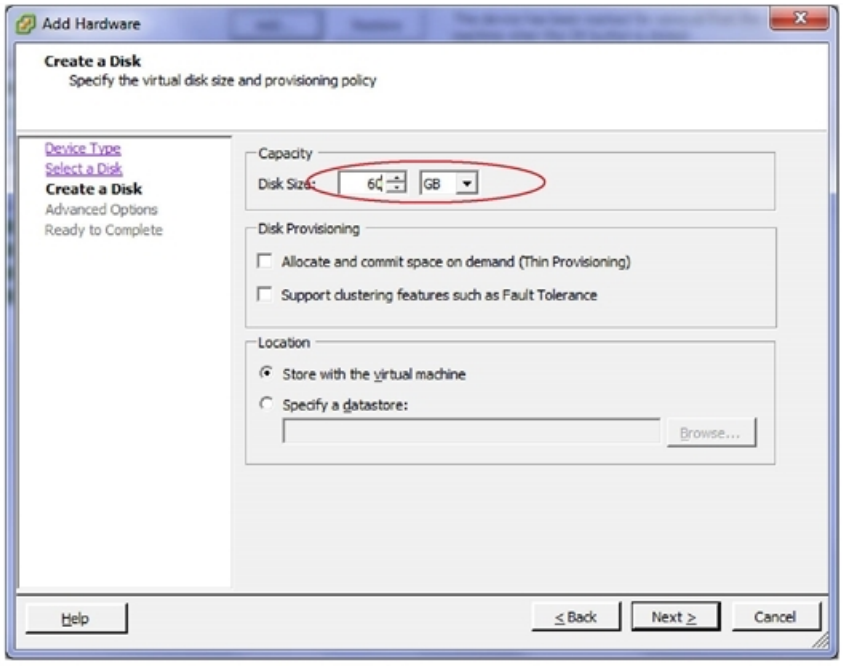
3. In the list of virtual hardware on the left side of the dialog, select **Hard disk 2** and click **Remove**.
4. Click **Add** to display the Add Hardware dialog.



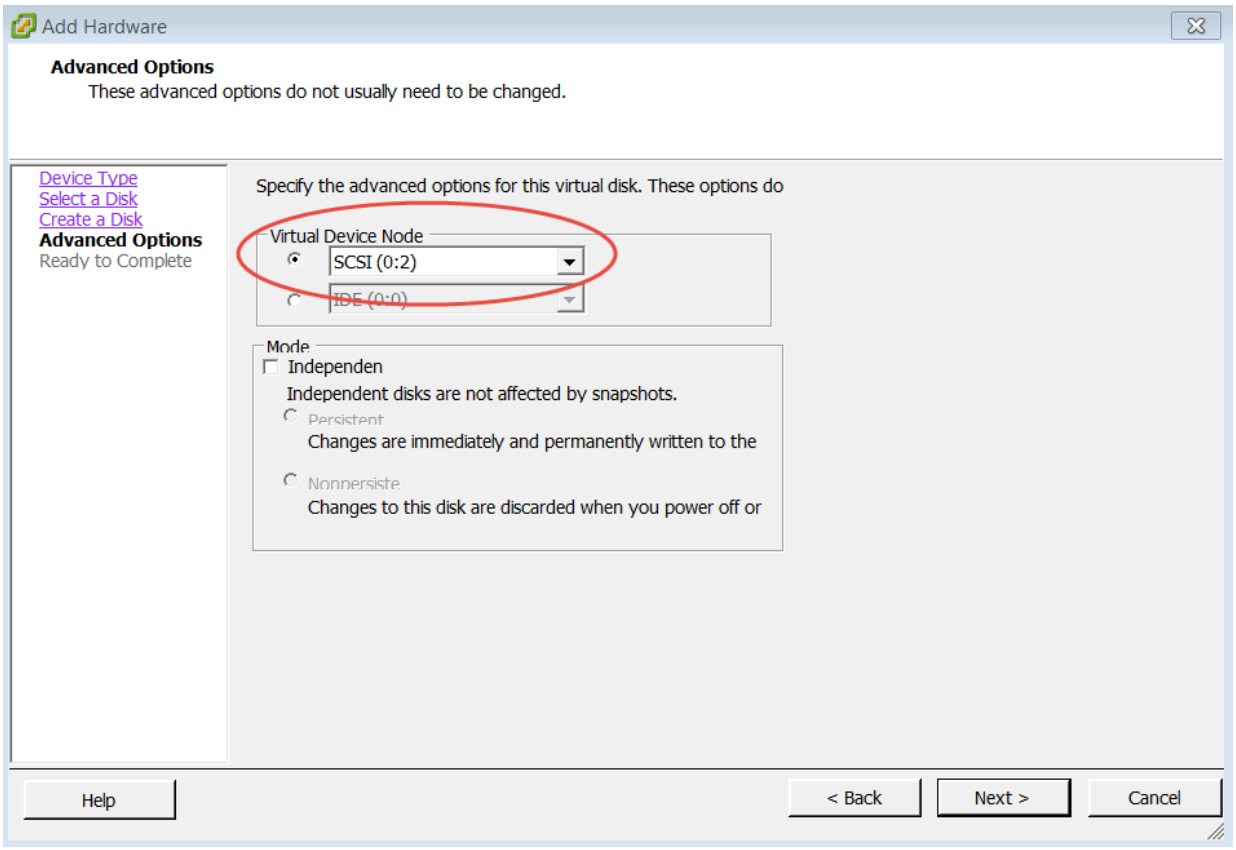
5. In the list of device types, click **Hard Disk** and then click **Next** to continue.
6. Select **Create a new virtual disk** and then click **Next** to continue.



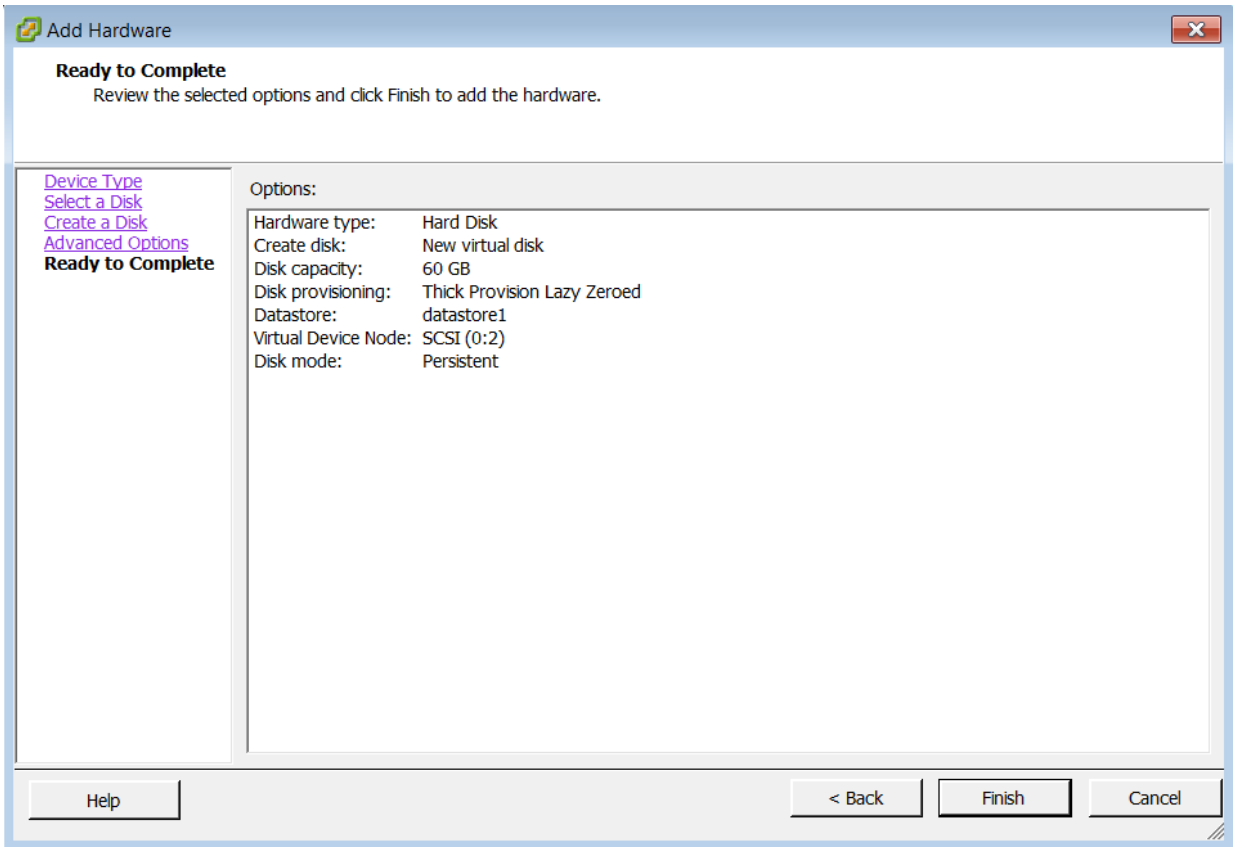
7. In Disk Size, type the new size, in gigabytes (GB), of the vDisk and then click **Next** to continue.



8. In Virtual Device Node, select **SCSI (0:2)** and then click **Next** to continue.



9. Review the configuration and click **Finish**.



10. Click **OK** to dismiss the Edit Settings dialog.

Configuring the number of virtual CPUs (vCPUs)

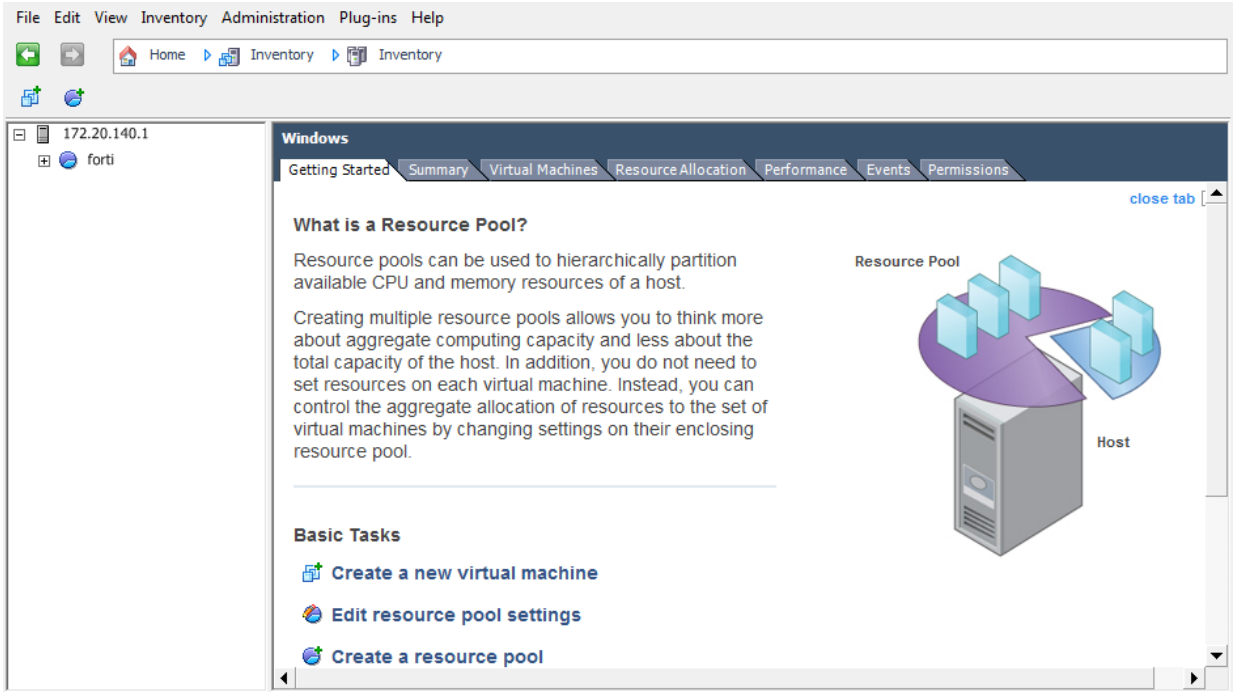
By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiADC-VM license that you purchased, you can allocate 1, 2, 4, or 8 vCPUs.

For more information on vCPUs, see the VMware vSphere documentation:

https://www.vmware.com/support/vsphere-hypervisor.html

To change the number of vCPUs:

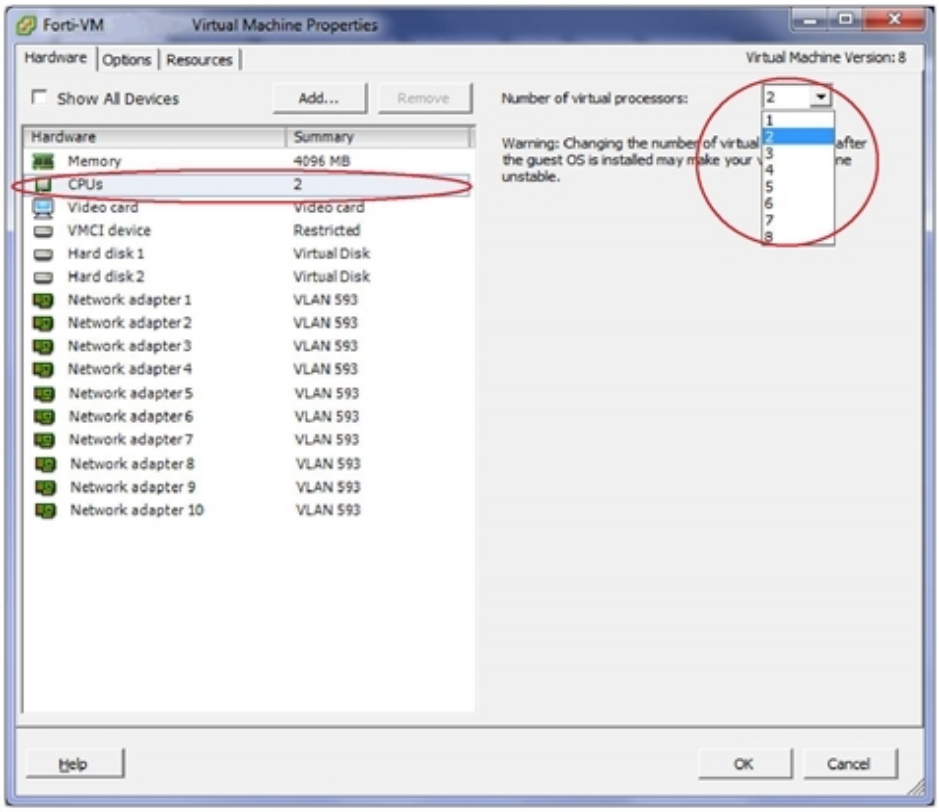
1. Use the VMware vSphere client to connect to VMware vSphere server.
   The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**.

   The virtual appliance properties dialog appears.

3. In the list of virtual hardware on the left side of the dialog, click **CPUs**.



4. In Number of virtual processors, specify the maximum number of vCPUs to allocate. Valid values range from 1 to 8.
5. Click **OK**.

Configuring the virtual RAM (vRAM) limit

The FortiADC-VM image is pre-configured to use 2 GB of vRAM. We recommend at least 4GB memory for all VM deployments. You can change this value. Appropriate values are suggested as follows, according to the number (n) of Layer-7 transactions that will be handled simultaneously by FortiADC-VM:

1 < n < 140,000 — 4 GB vRAM

140,001 < n < 300,000 —8 GB vRAM

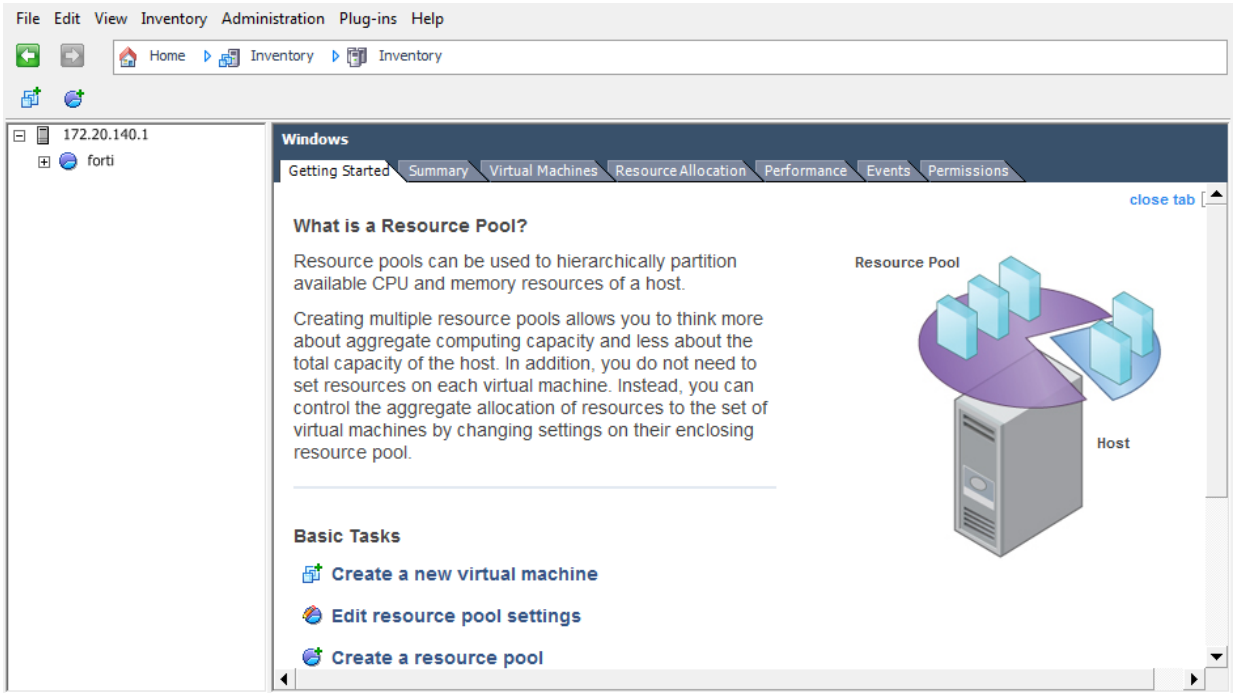
300,001 < n < 600,000 —16 GB vRAM

Also, sizing should be adjusted if the FortiADC-VM will be handling Layer-4 connections, or a mixture of Layer-4 and Layer-7 connections.

It is possible to configure FortiADC-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

To change the amount of vRAM:

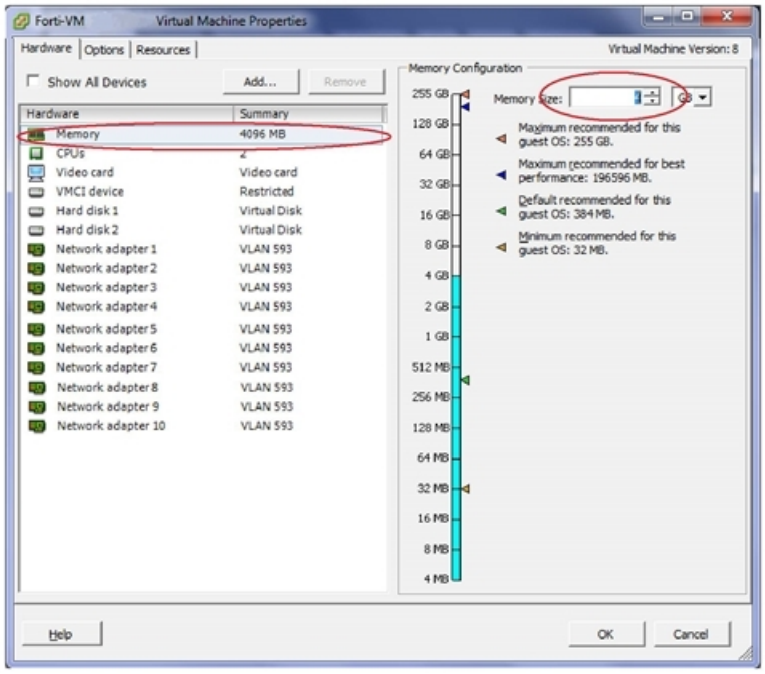
1. Use the VMware vSphere client to connect to VMware vSphere server.
   The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**.

The virtual appliance properties dialog appears.

3. In the list of virtual hardware on the left side of the dialog, click **Memory**.



4. In Memory Size, type the maximum number in gigabytes (GB) of the vRAM to allocate.
5. Click **OK**.

Mapping the virtual NICs (vNICs) to physical NICs

When you deploy the FortiADC-VM package, 10 bridging vNICs are created and automatically mapped to a port group on one virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 10 network interfaces in FortiADC-VM. (Alternatively, if you prefer, some or all of the network interfaces can be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if your VM environment requires it.

The appropriate mappings of the FortiADC-VM network adapter ports to the host computer physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and do not need to be changed.

If you are unsure of your network mappings, try bridging first before trying non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs.

Figure 4 illustrates how vNICs could be mapped to the physical network ports on a server.

Figure 4: Example: Network mapping

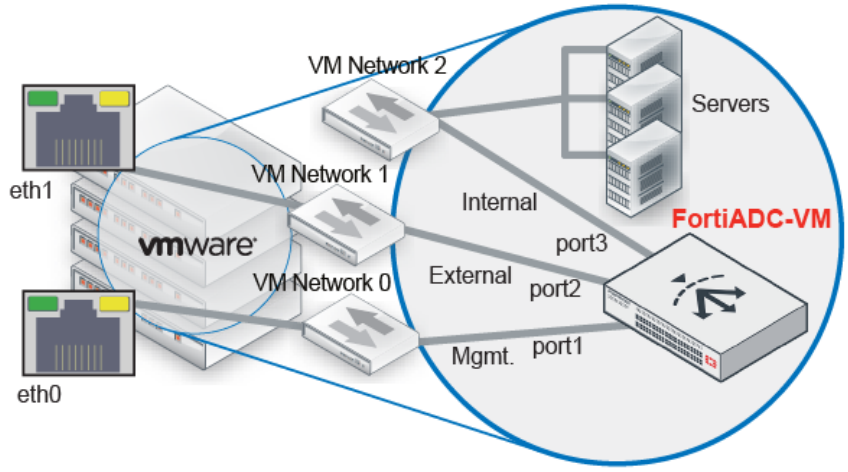
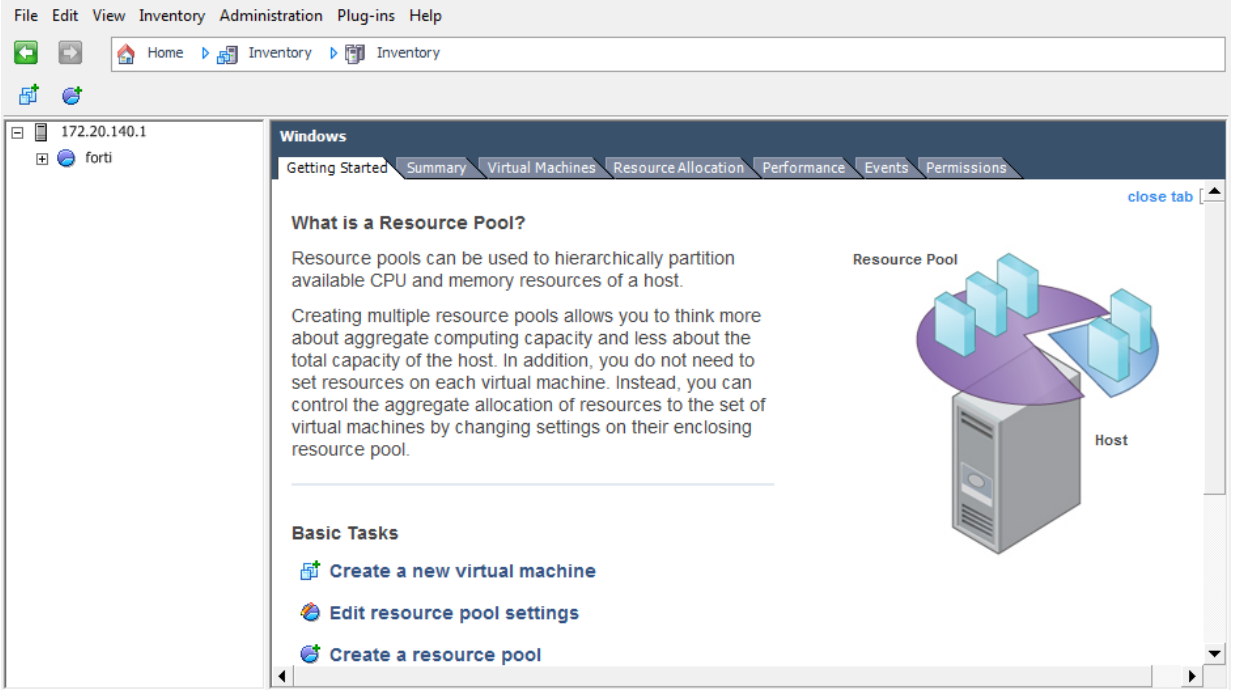


Table 3: Example: Network mapping

VMware vSphere			FortiADC-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiADC-VM**	**Network Interface Name in Web UI/CLI**
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
	VM Network 2	Internal	port3
			port4
			port5
			port6
			port7
			port8
			port9
			port10

To map network adapters:

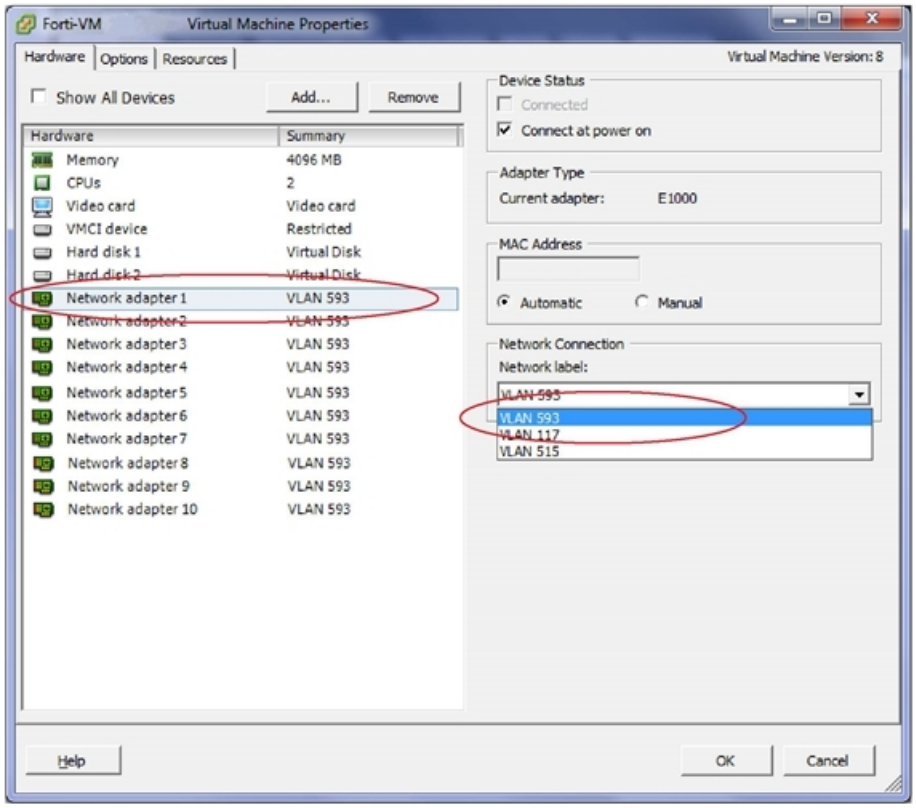
1. Use the VMware vSphere client to connect to VMware vSphere server.
   The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**.

   The virtual appliance properties dialog appears.

3. In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.



4. From the Network Connection drop-down menu, select the virtual network mapping for the virtual network adapter.

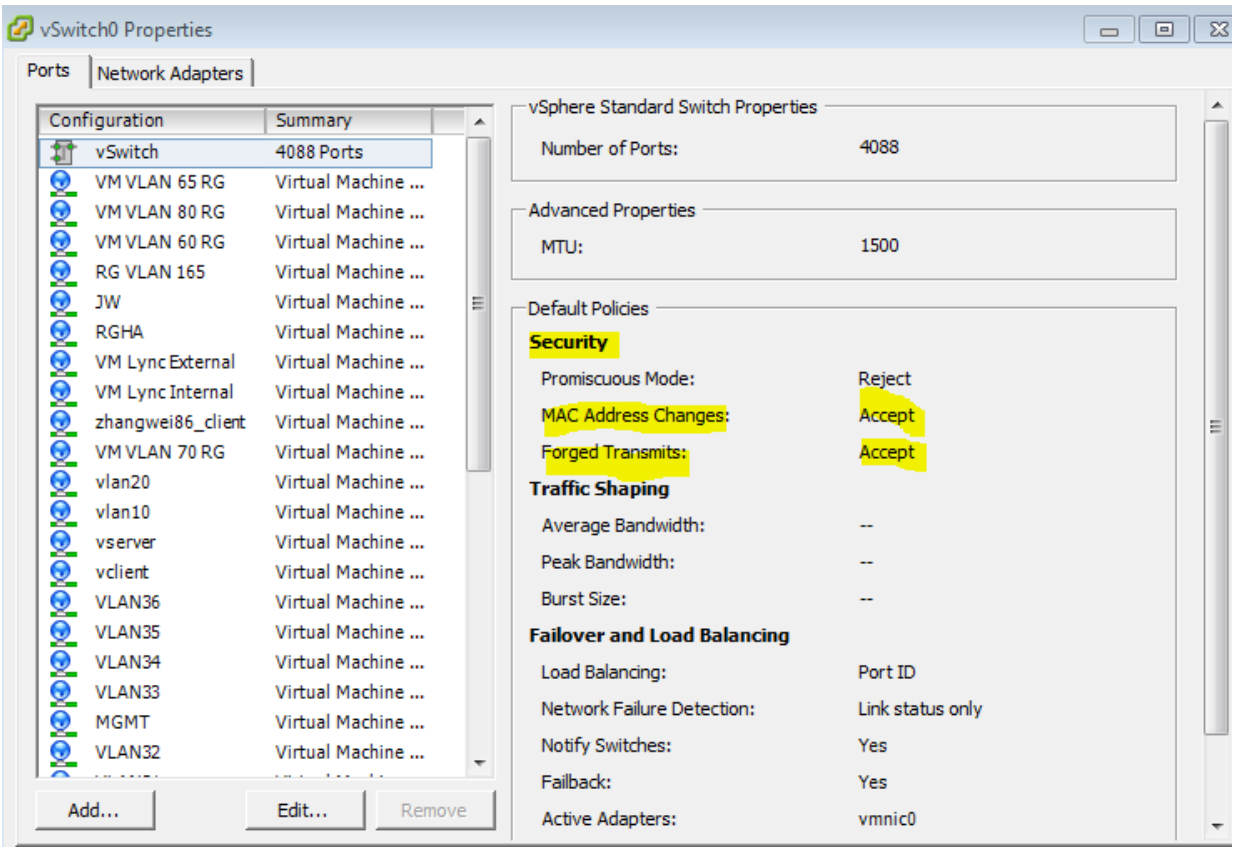
   The correct mapping varies by the virtual environment network configuration. In the example illustration above, the vNIC **Network adapter 1** is mapped to the virtual network (vNetwork) named **VLAN 593.**

5. Click **OK**.

HA Configuration

When configuring HA on FortiADC appliances using VMware VMs, ensure that the vSwitch can accept MAC Address Changes and Forced Transmits on the HA Heartbeat VLAN. For more information, see the FortiADC D-Series Handbook.

The illustration below shows what the vSwitch Properties page looks like with these settings enabled



Step 3: Power on the virtual appliance

After the virtual appliance software has been deployed and its virtual hardware configured, you can power on the virtual appliance.

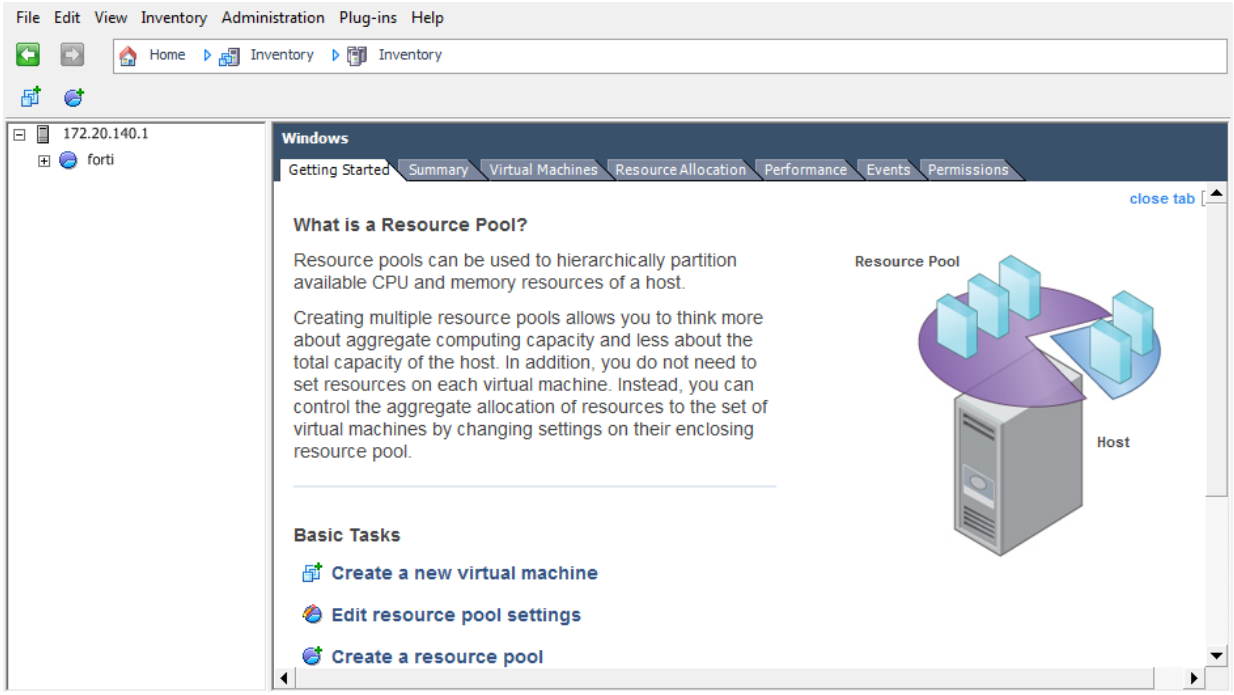
Before you begin:

- You must have resized the disk (VMDK).
- You must have resized the CPUs and RAM, if necessary.
- You must have mapped the virtual network adapters if the defaults are not appropriate.

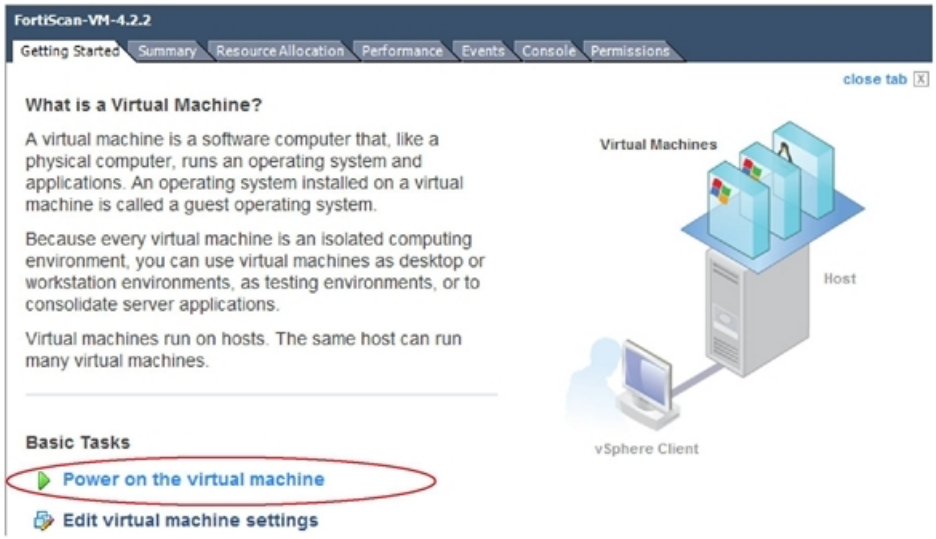
These settings must be configured in virtual machine environment. You do not configure them in the FortiADC OS.

To power on FortiADC-VM:

1. Use the VMware vSphere client to connect to VMware vSphere server.
   The following figure shows the vSphere client manager window.



2. In the left pane, click the name of the virtual appliance, such as **FortiADC-VM-Doc**.
3. Click the **Getting Started** tab.



4. Click **Power on the virtual machine**.

Step 4: Configure access to the web UI & CLI

Once it is powered on, you must log into the FortiADC-VM command-line interface (CLI) via the VMware vSphere console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. Use the VMware vSphere Client to log into the vSphere server.
2. In the left pane, select the name of the virtual appliance, such as **FortiADC-VM-Doc**.
3. Click the **Console** tab to open the console of the FortiADC-VM virtual appliance.
4. At the login prompt, type `admin` and no password to log in.
5. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit port1
      set ip <address/mask>
      set allowaccess {http https ping snmp ssh telnet}
end
config router static
   edit 1
      set gateway <gateway_address>
end
config system dns
   set primary <dns_address>
   set secondary <dns_address>
end
```

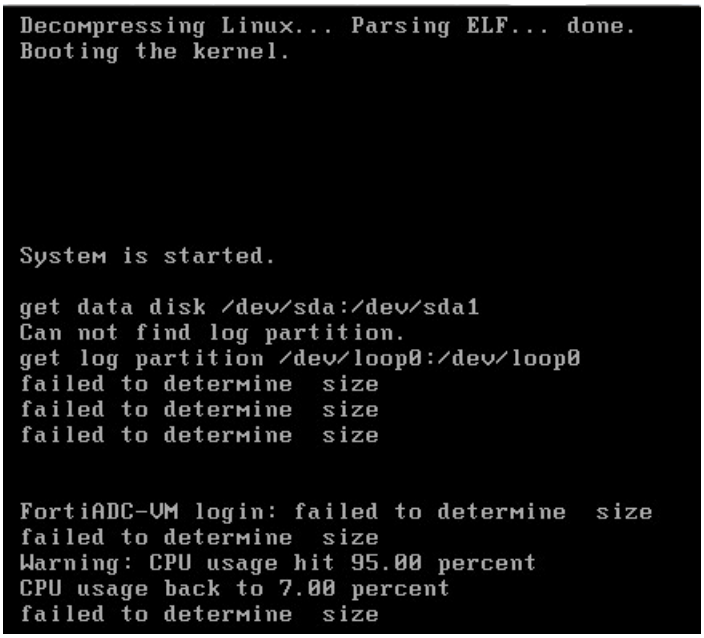
where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.
- `<gateway_address>}` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

Important: If you upgrade the vDisk size, the vDisk size and FortiADC-VM log partition size likely do not match, and you will see the disk errors shown in the following figure when you attempt to log into the console.



To fix this:

1. Press Enter repeatedly until you see the login prompt.
2. At the login prompt, type `admin` and no password to log in.
3. Enter the following command to fix the disk issue:

```
execute formatlogdisk
```

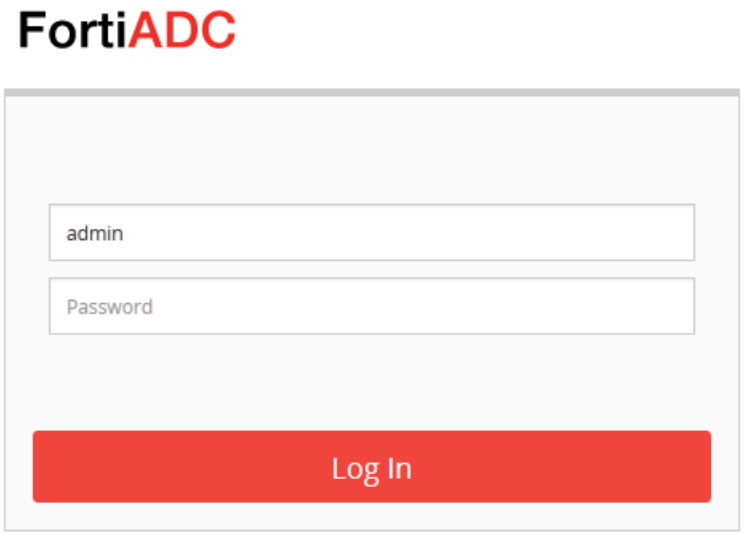
Step 5: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

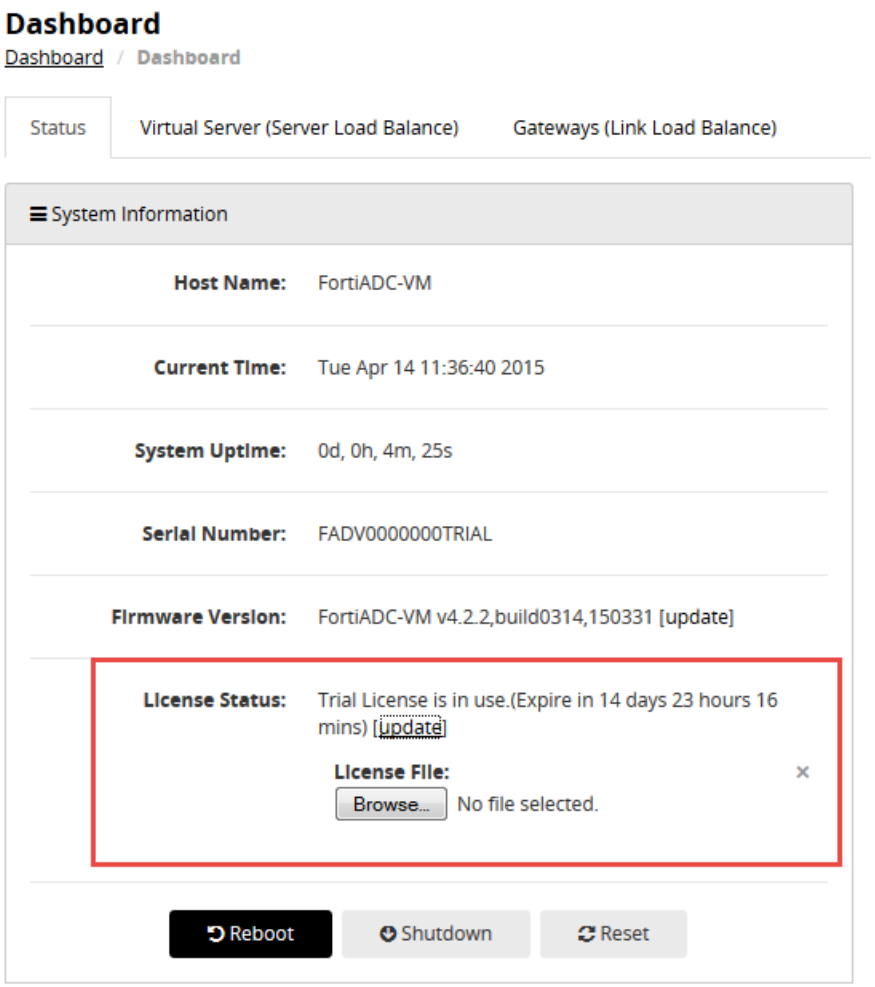
You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as: `https://192.168.1.99/`.
   The web UI login page appears.



3. Use the username `admin` and no password to log in.
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The web UI opens to the dashboard.
5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

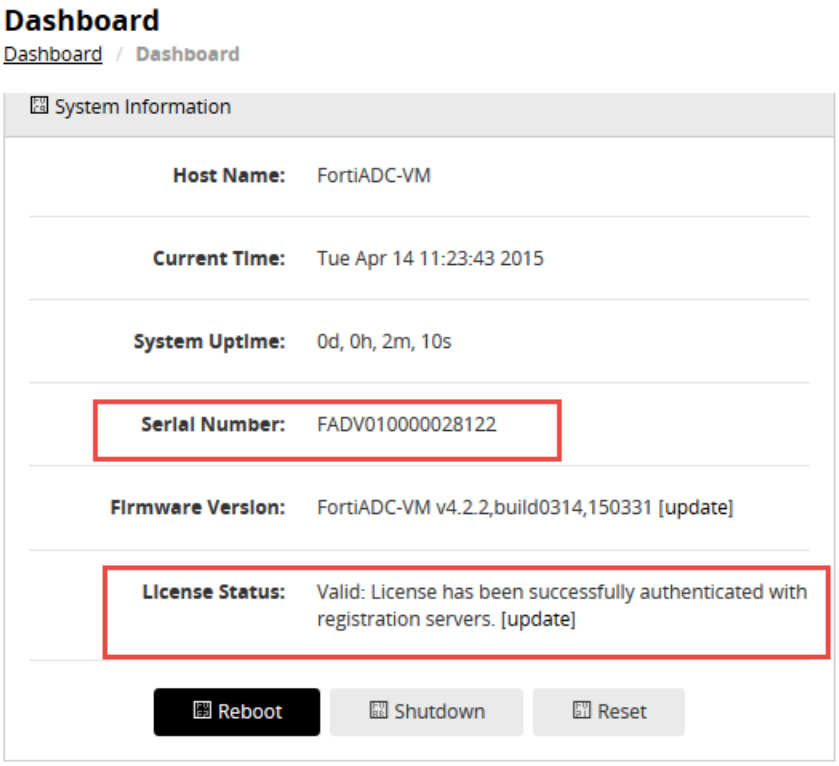


After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```



If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
```

```
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

What's next?

At this point, the FortiADC virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the *FortiADC Handbook* for information on getting started with feature configuration.

Upgrading the number of VM CPUs

FortiADC-VM is licensed for either 1, 2, 4, or 8 CPUs. If you start with one license and outgrow it, you can upgrade.

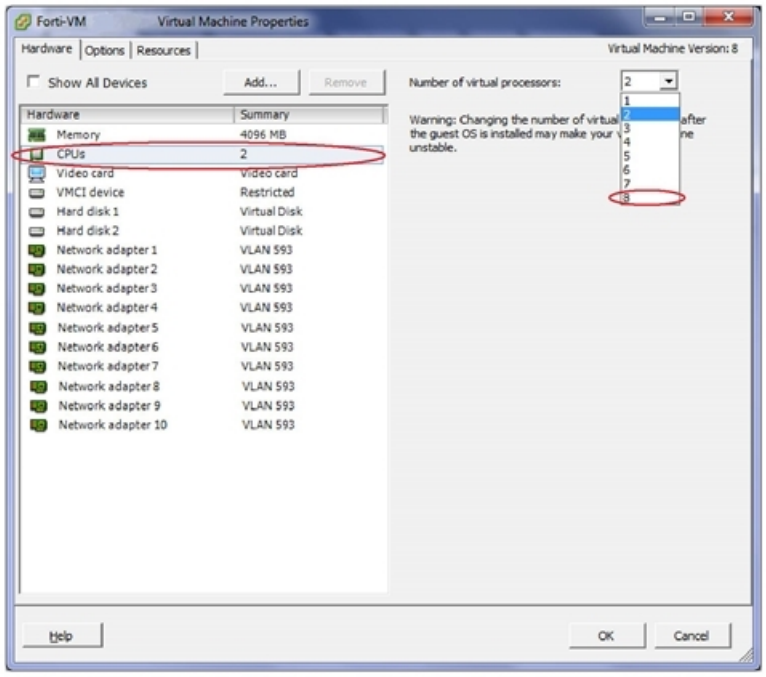
Before you begin:

- You must purchase the new license and copy the license file to your management computer.
- Be aware that you must shut down FortiADC and power off the virtual machine to perform the upgrade.

To allocate more vCPUs:

1. In the FortiADC web UI, go to System > Status > Dashboard.
2. Upload the new license. For details, see Step 5: Upload the license file.
3. In the System Information widget, click **Shut Down**.
   The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiADC-VM, you might lose buffered data.
4. On your management computer, log into the vSphere server.

5. In the left pane, click the name of the virtual appliance, such as **FortiADC-VM-Doc**.
6. Click the **Getting Started** tab.
7. Click **Power off the virtual machine**.
8. Increase the vCPU allocation. For details, see Configuring the number of virtual CPUs (vCPUs).



9. Power on the virtual appliance again.

Upgrading the virtual hardware

By default, the FortiADC-VM fortiadc-vm-64-hw7.ovf image uses VMware virtual hardware version 7. If you have a VMware ESXi 5.1 environment that supports virtual hardware version 9, and you want to provide version 9 feature support such as backups, you can update the virtual hardware.

For more information on virtual hardware, see:

http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675

To upgrade the virtual hardware:

1. Shut down FortiADC-VM. To do this, you can enter the CLI command:

   ```
   execute shutdown
   ```

2. In VMware vCenter, right-click the VM and select **Power > Power Off.**
3. After it has been powered off, right-click the VM and select the option to upgrade the virtual hardware.
4. When the upgrade is complete, power on FortiADC-VM.

Chapter 3: Deploying FortiADC-VM on Microsoft Hyper-V

This chapter provides procedures for FortiADC-VM on Microsoft Hyper-V. It includes the following information:

Installation overview

You deploy FortiADC-VM on Microsoft Hyper-V by importing a virtual machine.

Before you begin:

- You must have already installed Windows Server 2012 R2 and enabled Hyper-V. Refer to Microsoft documentation for instructions:
  - https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012
  - https://technet.microsoft.com/en-us/library/hh846766.aspx
- **Tip**: To quickly use remote desktop to control Hyper-V server, turn on the remote desktop function and turn off the firewall on the server side:

```
netsh advfirewall set allprofiles state on
```

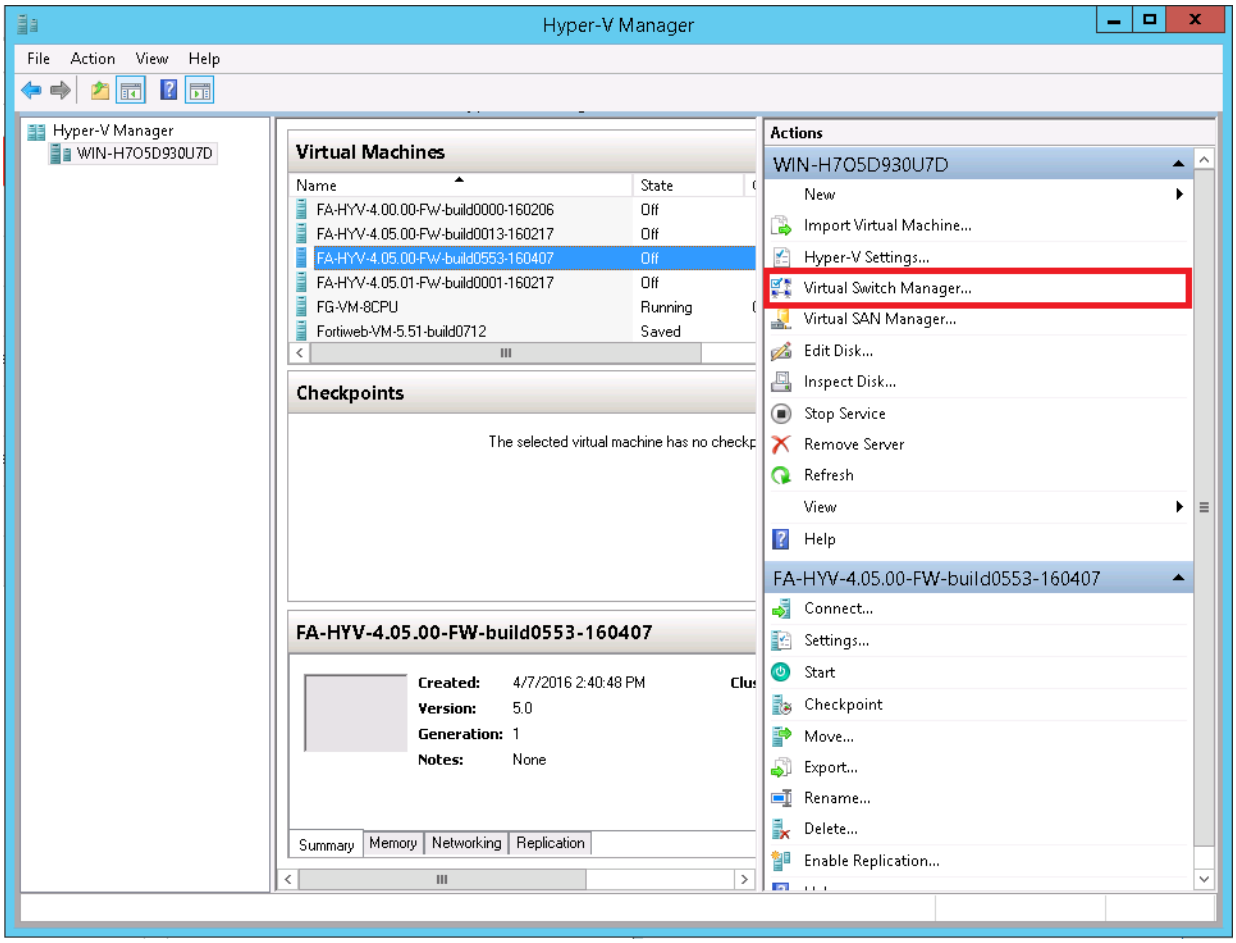
Step 1: Import the FortiADC-VM virtual machine

Before you begin:

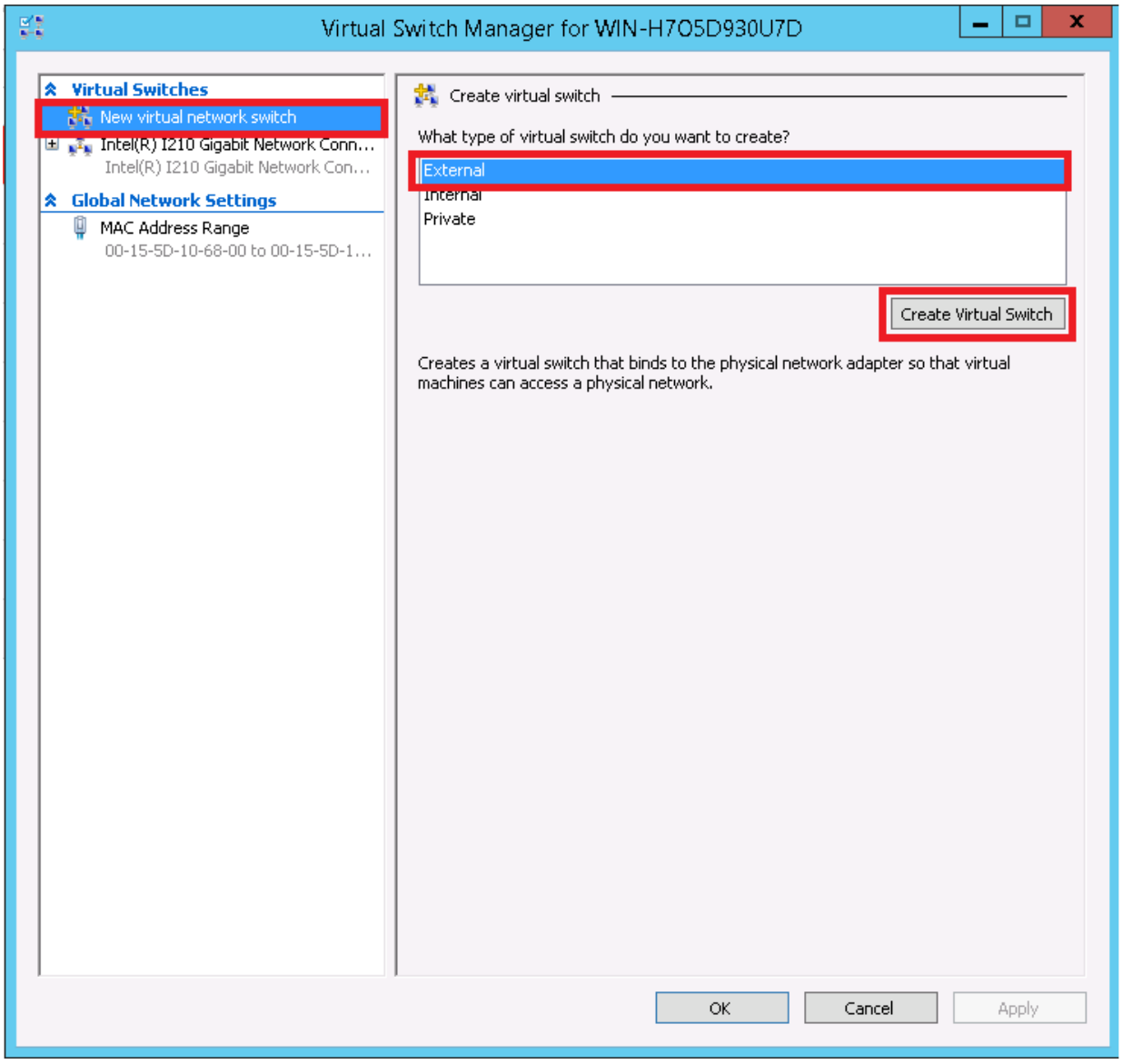
- Extract the contents of the FortiADC-VM image .zip file to a folder that you can access from the Hyper-V Manager.
- The instructions in this section create a virtual switch named `vmnet`. The FortiADC-VM virtual machine you import uses a virtual switch with this name by default. Alternatively, you can use an existing virtual switch or one with different name. You are prompted to select the switch you want to use when you import the virtual machine.

To import the FortiADC-VM virtual machine:

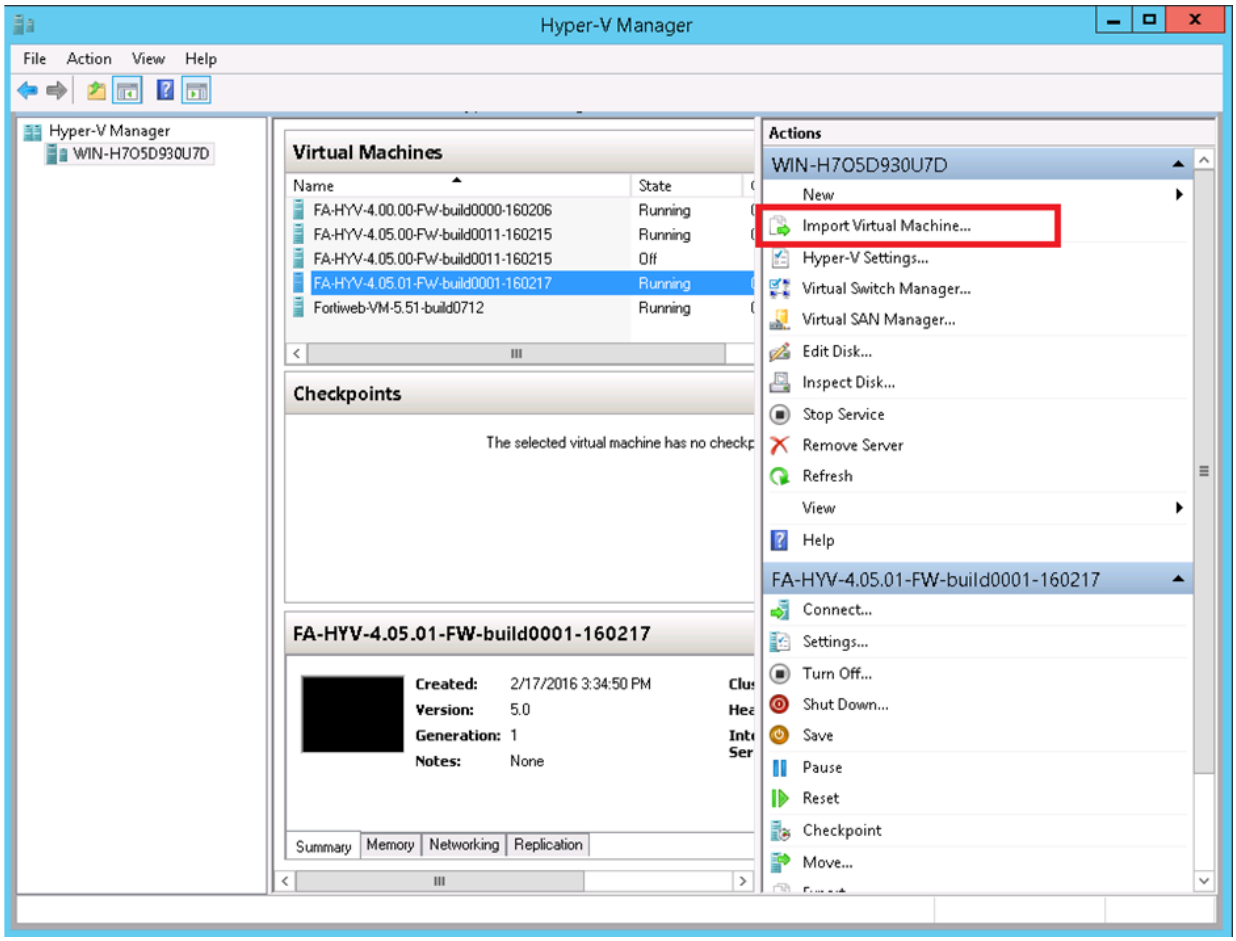
1. In the Hyper-V Manager, under Actions, click **Virtual Switch Manager**.



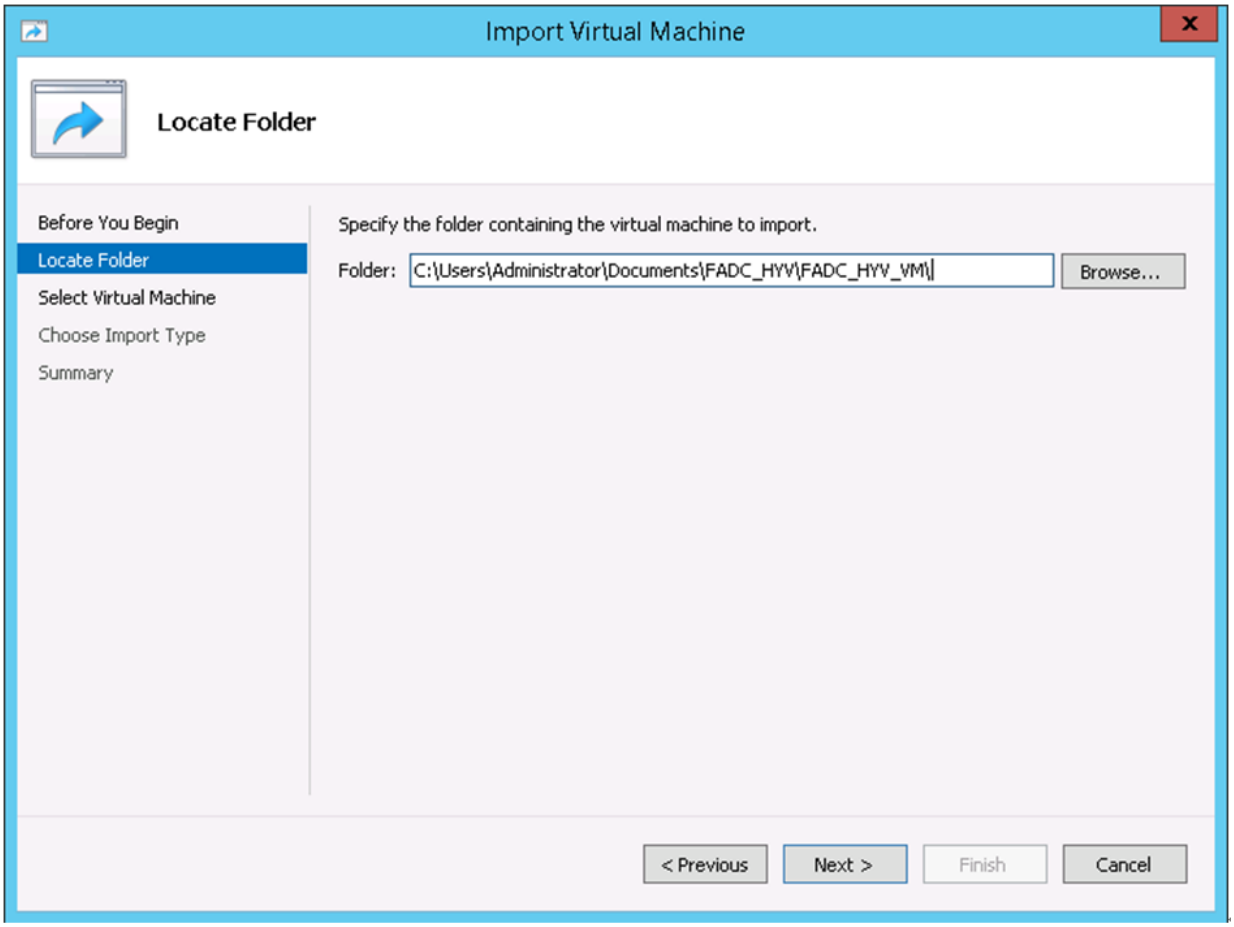
2. Under Virtual Switches, click **New virtual network switch**, click **External**, and then click **Create Virtual Switch**.



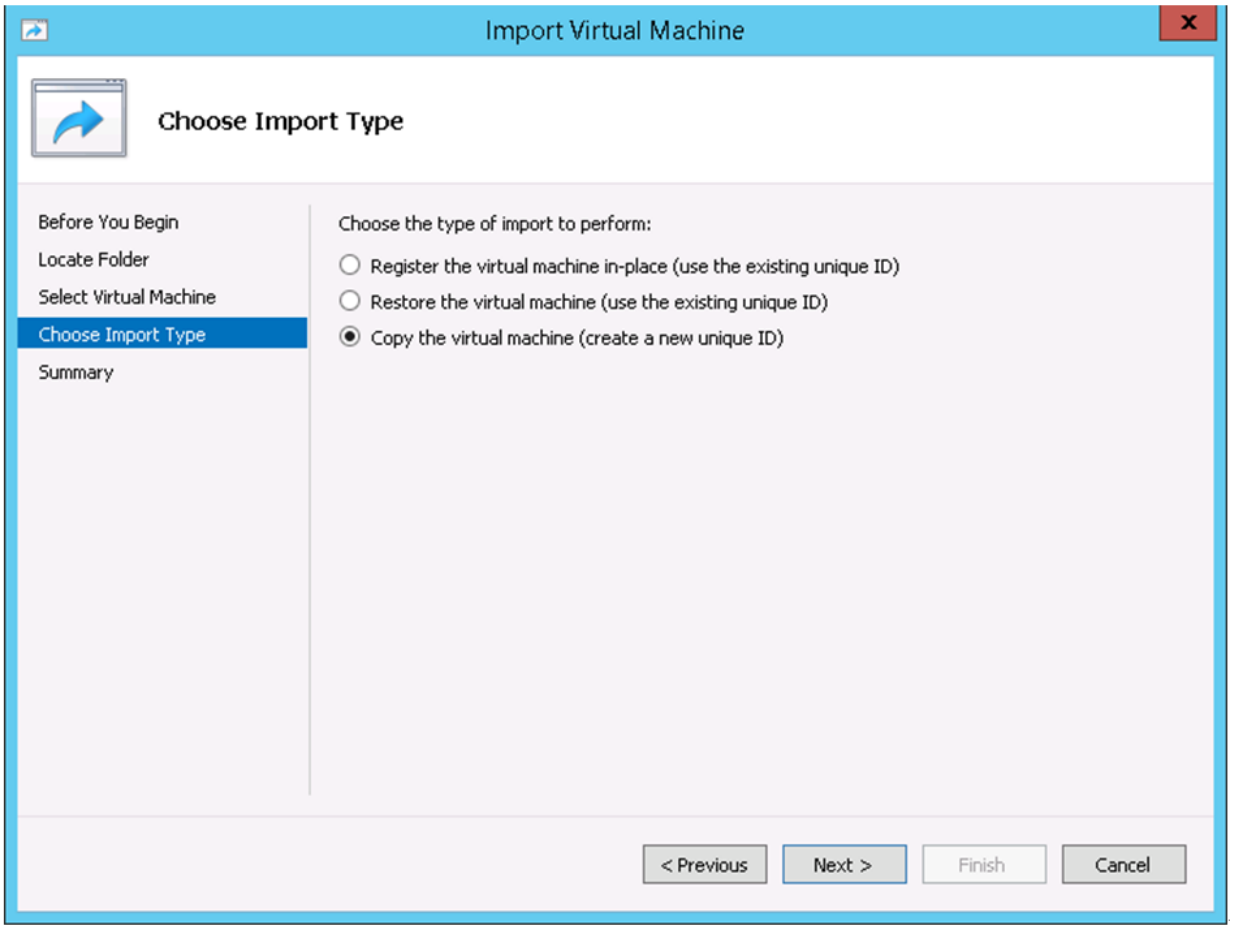
3. Under Virtual Switch Properties, for Name, enter `vmnet`. For all other settings, use the default values.
4. Click **OK**.
5. In Hyper-V Manager, under Actions, click **Import Virtual Machine**.



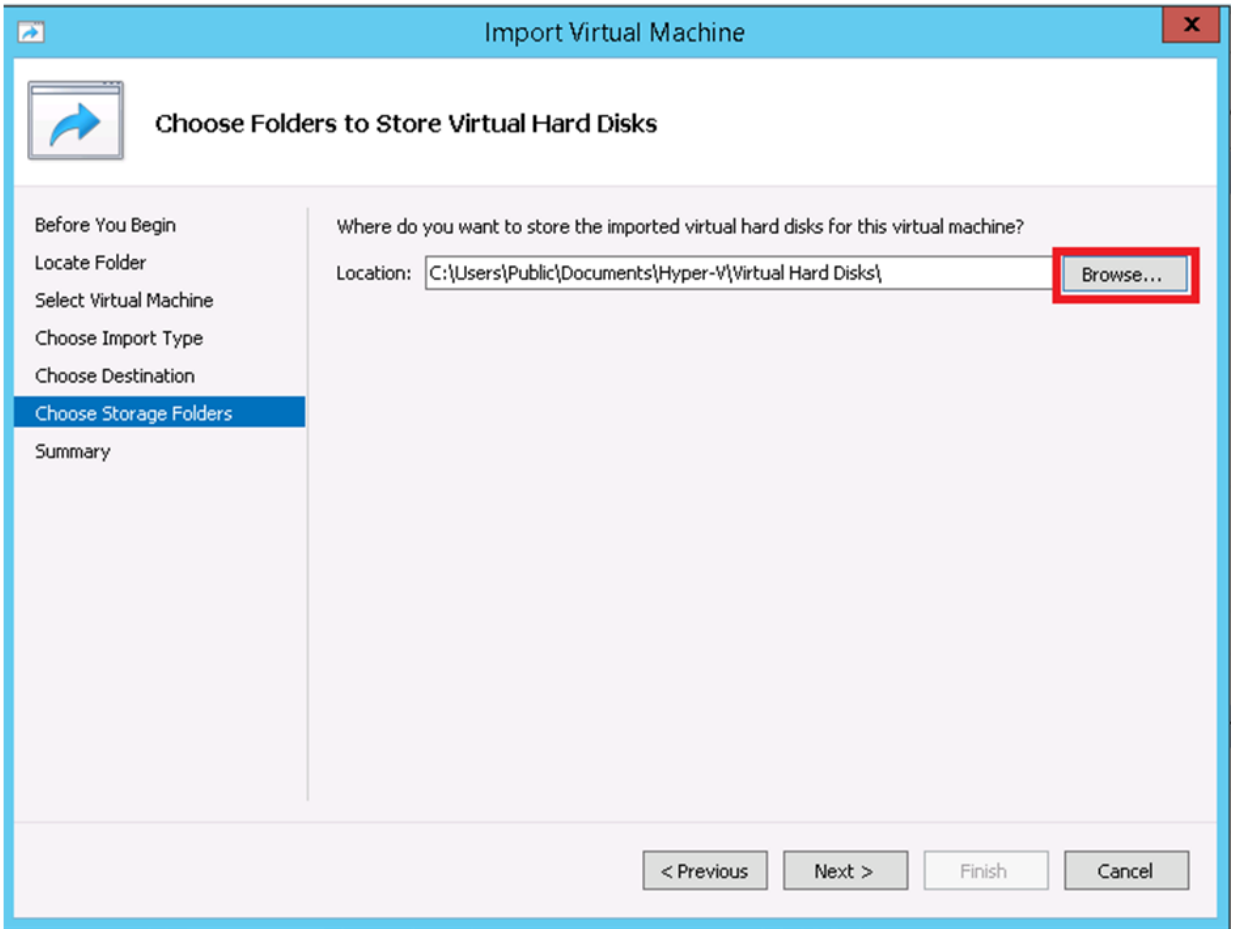
6. In the Import Virtual Machine wizard, navigate to the Locate Folder page.



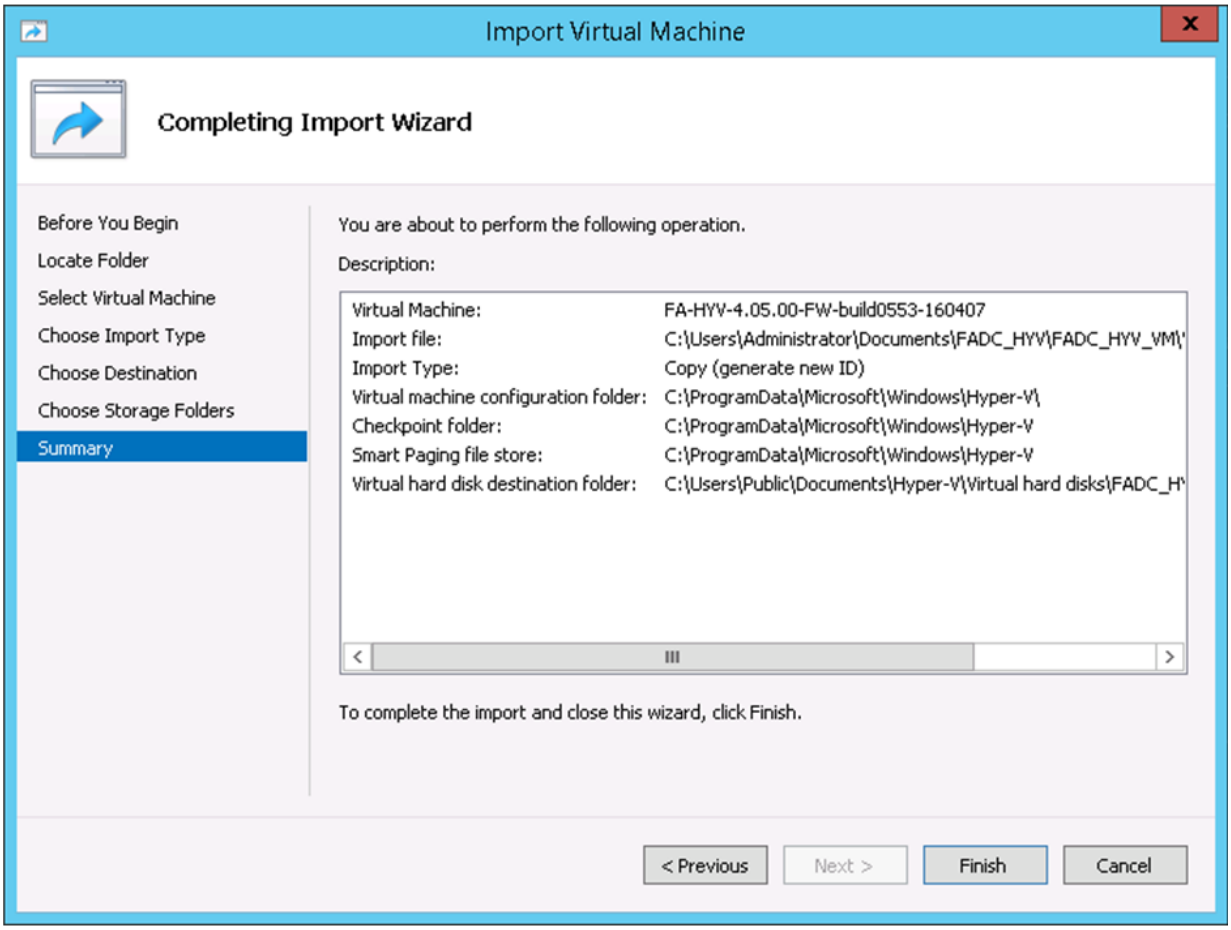
7. For Folder, specify the folder that contains the contents of the .zip file, and then click **Next**.
8. On the Select Virtual Machine page, select the name of the FortiADC-VM virtual machine, and then click **Next**.
9. On the Choose Import Type page, select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.



10. On the Choose Folders to Store Virtual Hard Disks page, preserve the default values or specify the folders where you want to store the virtual machine. Then, click **Next**.



11. On the Completing Import Wizard page, review the settings, and then click **Finish**.



Step 2: Configure virtual hardware settings

After deploying the FortiADC-VM image and before powering on the virtual appliance, log into the Hyper-V Manager and configure the virtual appliance hardware settings to suit the size of your deployment.

Table 4 summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Table 4: Virtual hardware settings

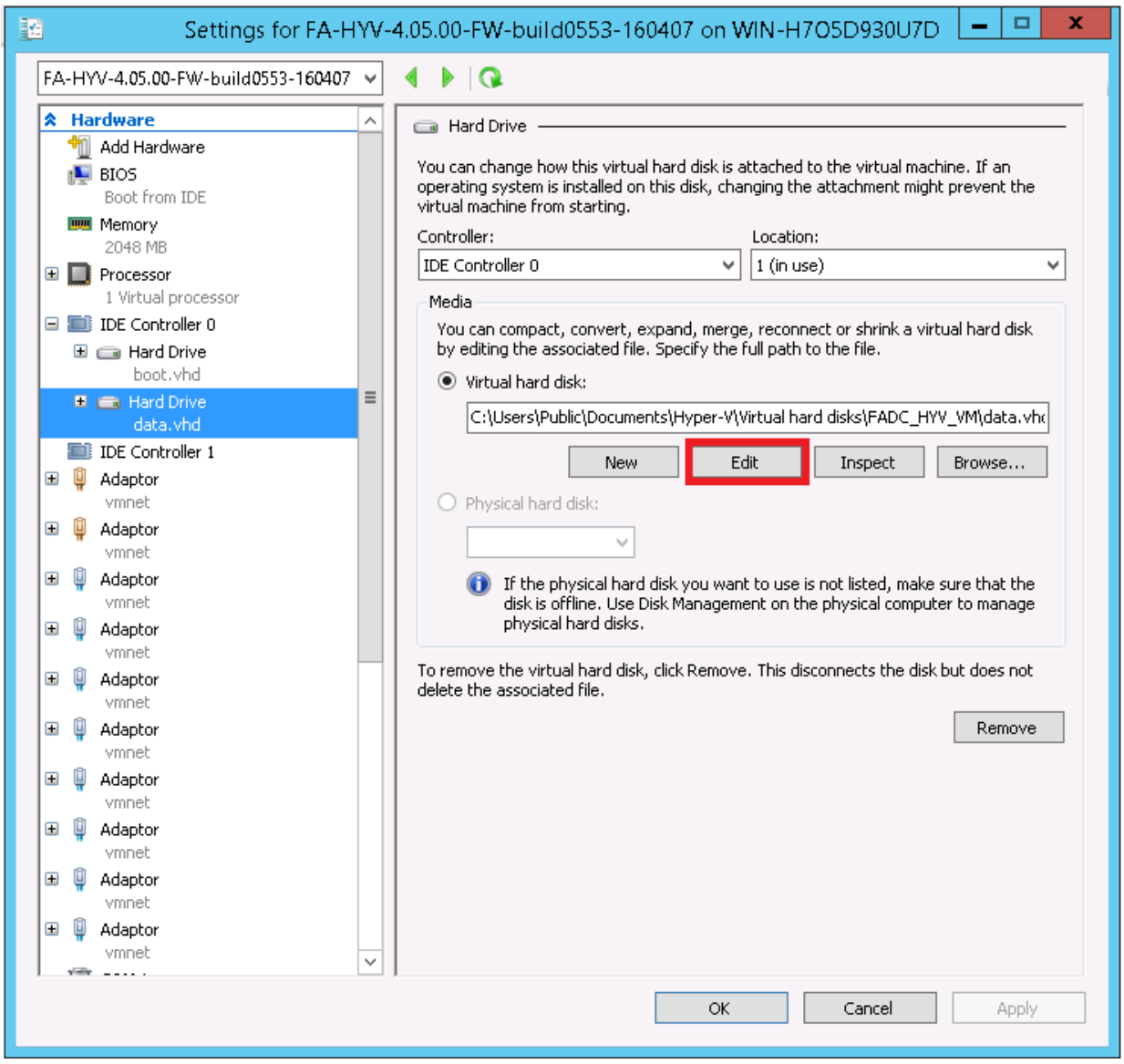
Component	Default	Guidelines
Hard drive	30 GB	30 GB is insufficient for most deployments. You must upgrade the hard drive before you power on the appliance. After you power on the appliance, you must reformat the FortiADC OS log disk with the following command: `execute formatlogdisk`
CPU	1 CPU	1 CPU is appropriate for a VM01 license. Upgrade to 2, 4, or 8 CPU for VM02, VM04, and VMO8 licenses, respectively.
RAM	2 GB	2 GB is the minimum. See the section on vRAM for guidelines based on expected concurrent connections.
Network interfaces	10 bridging vNICs are mapped to a port group on one virtual switch (vSwitch).	Change the mapping as required for your VM environment and network.

Resizing the virtual disk

The virtual disk size of the imported FortiADC-VM virtual machine is 30 GB (the default size for a Hyper-V virtual machine).

To increase the size of the virtual hard disk:

1. Shut down the FortiADC-VM virtual machine (**Actions > Shut Down**).
2. Select the FortiADC-VM virtual machine in the list of machines, and then, under Actions, click **Settings**.
3. Under Hardware, expand the IDE Controller item that contains the machine's hard drives, and then select the hard drive `data.vhd`.



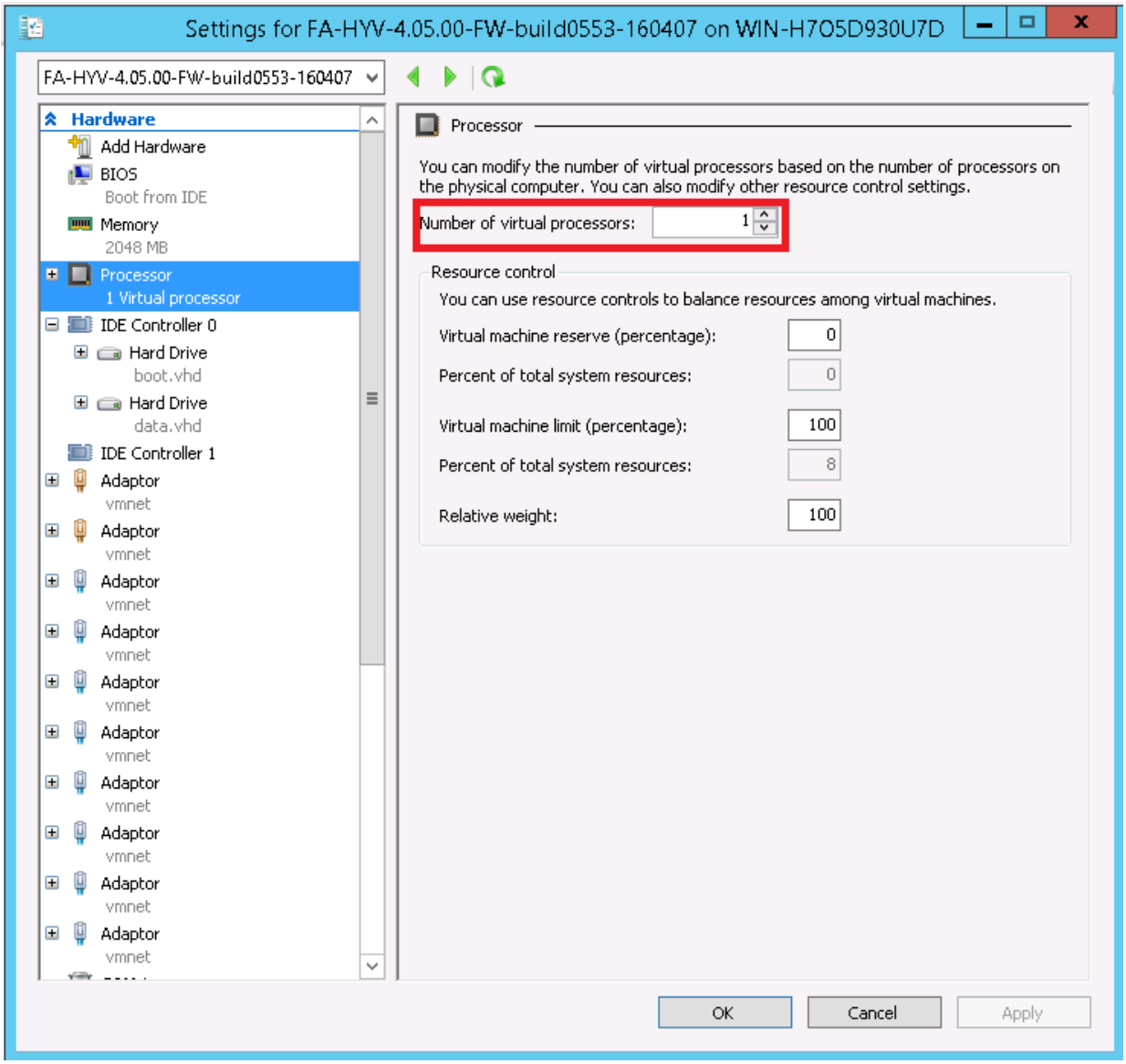
4. In the hard drive settings, under Media, ensure that **Virtual hard disk** is selected, click **Edit**, and then use the Edit Virtual Hard Disk wizard to expand the size of the virtual disk.
5. Start the virtual machine (**Actions > Start**).

Configuring the number of virtual CPUs (vCPUs) and RAM

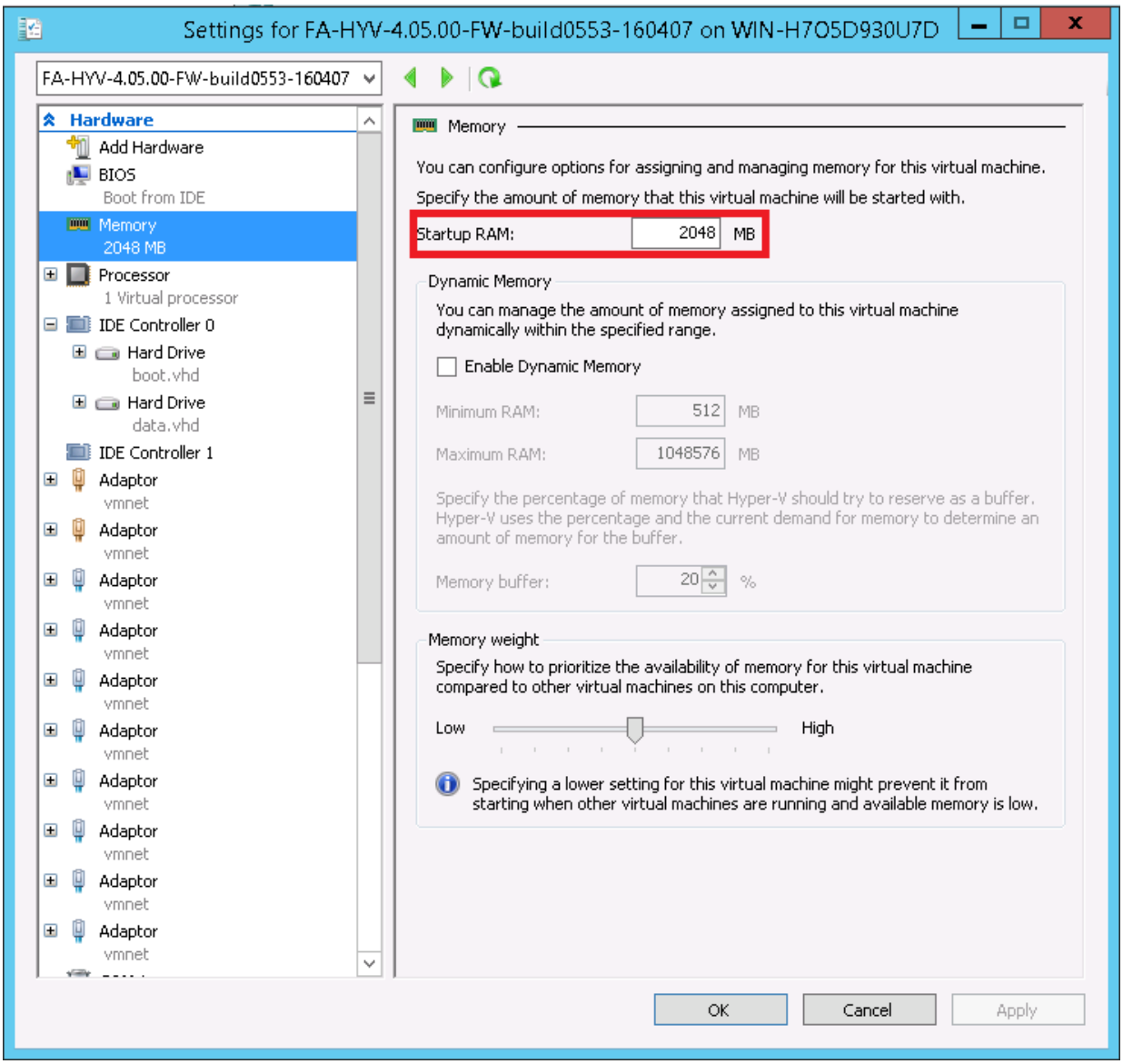
By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiADC-VM license that you purchased, you can allocate from 1 to 8 vCPUs.

To change the number of vCPUs and RAM:

1. Shut down the virtual machine (**Actions > Shut Down**).
2. Select the FortiADC-VM virtual machine in the list of machines, and then, under Actions, click **Settings**.
3. Under Hardware, select the **Processor** item, and then use the Processor settings to increase or decrease the number of vCPUs.



4. Under Hardware, select the **Memory** item, and then use the Memory settings to increase or decrease the Startup RAM.

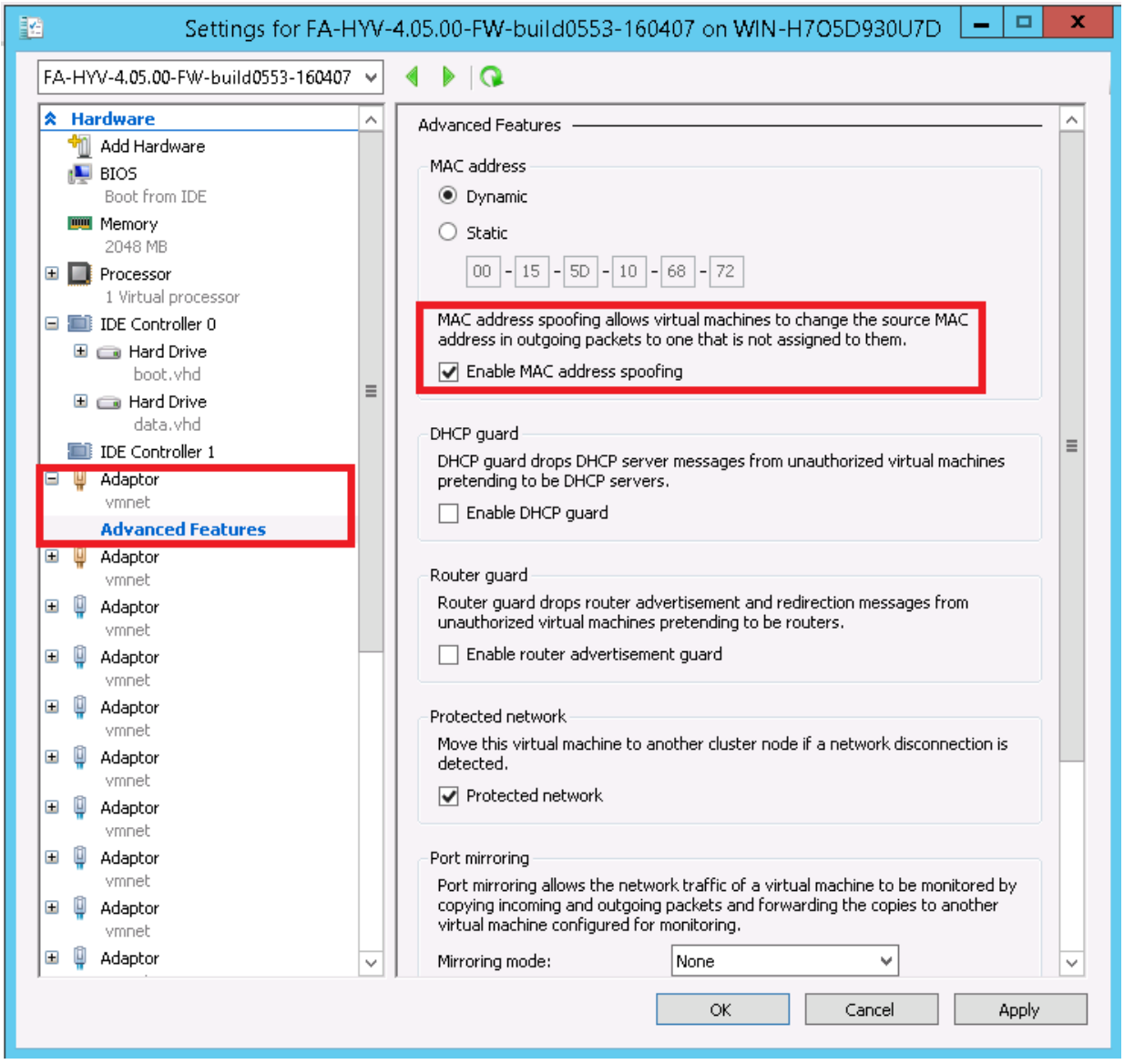


5. Click **OK** and then start the machine.

MAC address spoofing

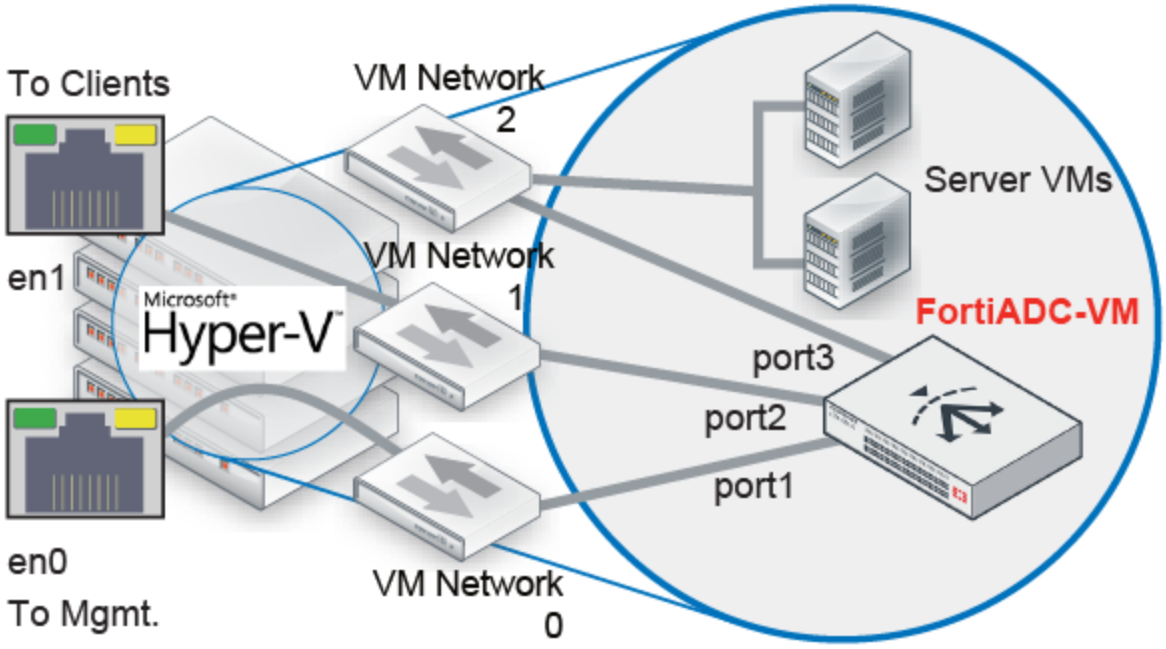
To operate correctly, FortiADC-VM virtual switches require MAC address spoofing. The option is enabled by default when you create a virtual switch. It is located in the settings for the virtual machine under Hardware. To view the option, simply expand the virtual switch component and then select **Advanced Features**.

Important: In order for the HA feature to work correctly, the Hyper-V HA setup also requires that the virtual switch connecting the heartbeat port also have MAC address spoofing configured.



Mapping the virtual NICs (vNICs) to physical NICs

When you import the FortiADC-VM package, the import process creates 10 bridging vNICs and automatically maps them to a port group on 1 virtual switch (vSwitch) within the hypervisor (the default name of this vSwitch is `vmnet`). Each of the 10 network interfaces in FortiADC-VM uses one of these vNICs. vSwitches are themselves mapped to physical ports on the server.



In most cases, you do not need to change the default mappings of the FortiADC-VM network adapter ports to the host computer's physical ports. The default bridging vNIC mappings are appropriate for configurations where each of the host's guest virtual machines have their own IP addresses on your network.

You can change the mapping, map other vNICs, or create additional vSwitches, if your VM environment requires it.

To configure the mappings, in the Hyper-V Manager, go to Actions > Virtual Switch. Manager.

If you are unsure of your network mappings, try bridging before you attempt non-default vNIC modes such as NAT or host-only networks.

Step 3: Start the FortiADC-VM

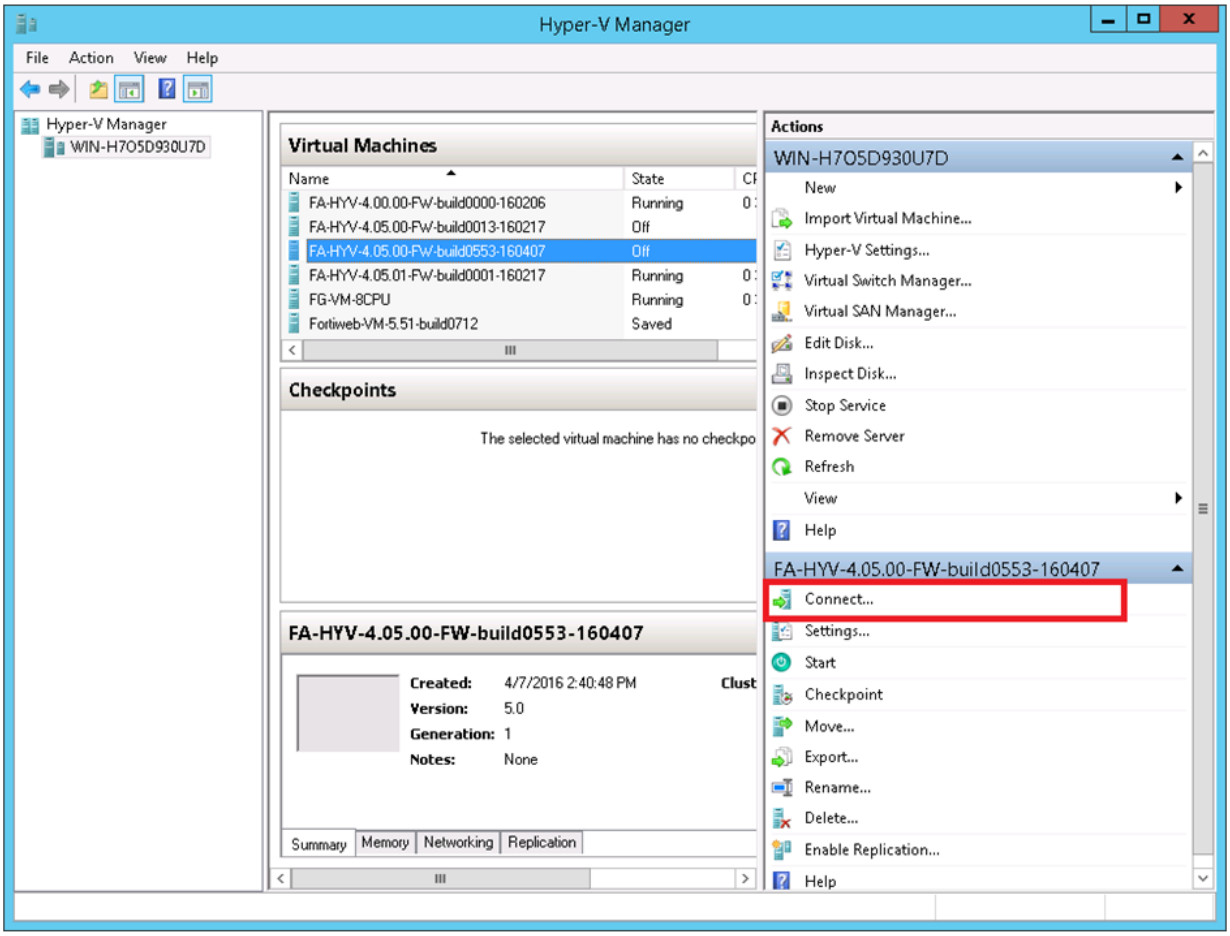
You can now power on the FortiADC-VM. Select the name of the FortiADC-VM in the list of virtual machines, right-click, and select **Start**.

Step 4: Configure access to the web UI & CLI

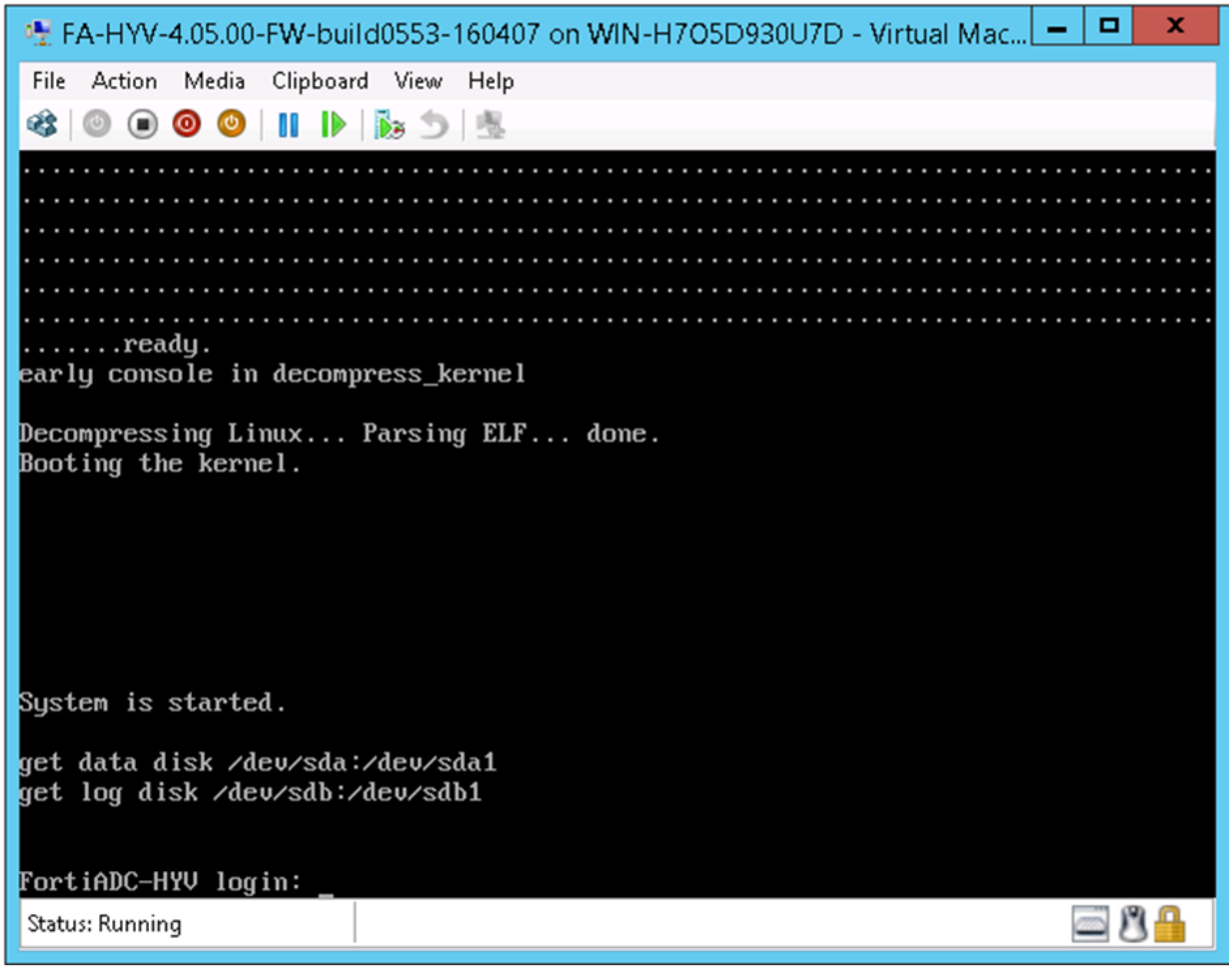
Once it is powered on, you must log in to the FortiADC-VM command-line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. In the Hyper-V Manager, under Virtual Machines, right-click the name of the virtual machine and select **Connect** to connect to the console.



The console shows the boot process.



2. At the login prompt, type `admin` and no password to log in.
3. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit port1
      set ip <address/mask>
      set allowaccess {http https ping snmp ssh telnet}
end
config router static
   edit 1
      set gateway <gateway_address>
end
config system dns
   set primary <dns_address>
   set secondary <dns_address>
end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.

- `<gateway_address>}` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

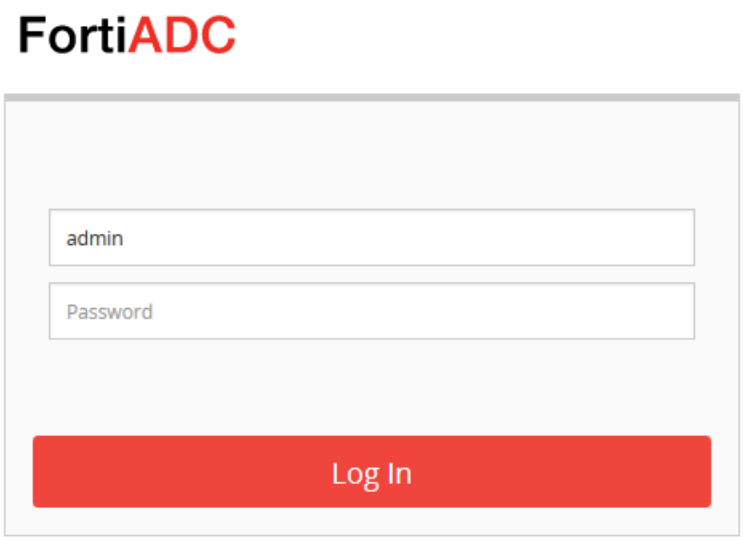
Step 5: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

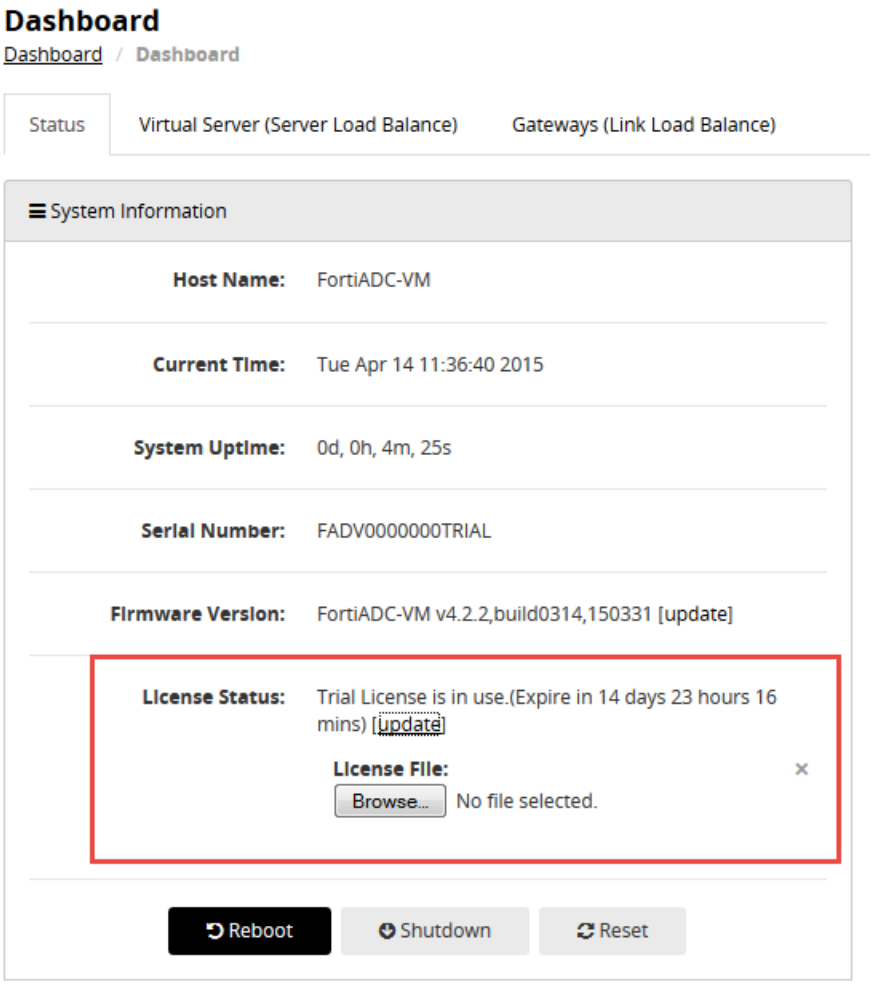
1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as: `https://192.168.1.99/`.
   The web UI login page appears.



3. Use the username `admin` and no password to log in.
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.

The web UI opens to the dashboard.

5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

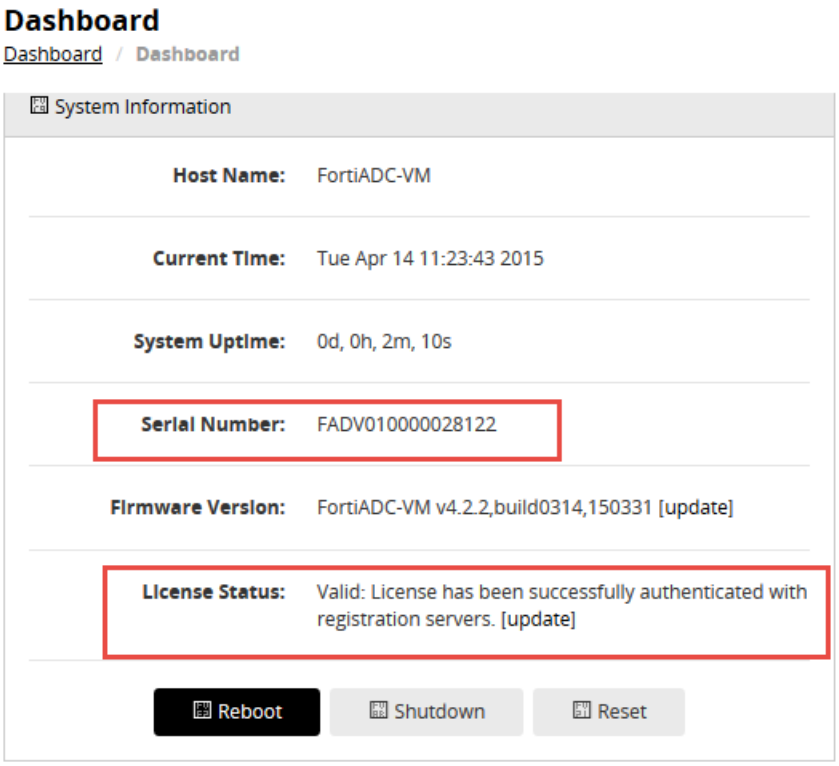


After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```



If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
```

```
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

What's next?

At this point, the FortiADC virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the *FortiADC Handbook* for information on getting started with feature configuration.

Chapter 4: Deploying FortiADC-VM on KVM

You deploy FortiADC-VM on kernel-based virtual machines (KVM) by importing a disk image. The workflow combines importing the image and configuring the VM hardware.

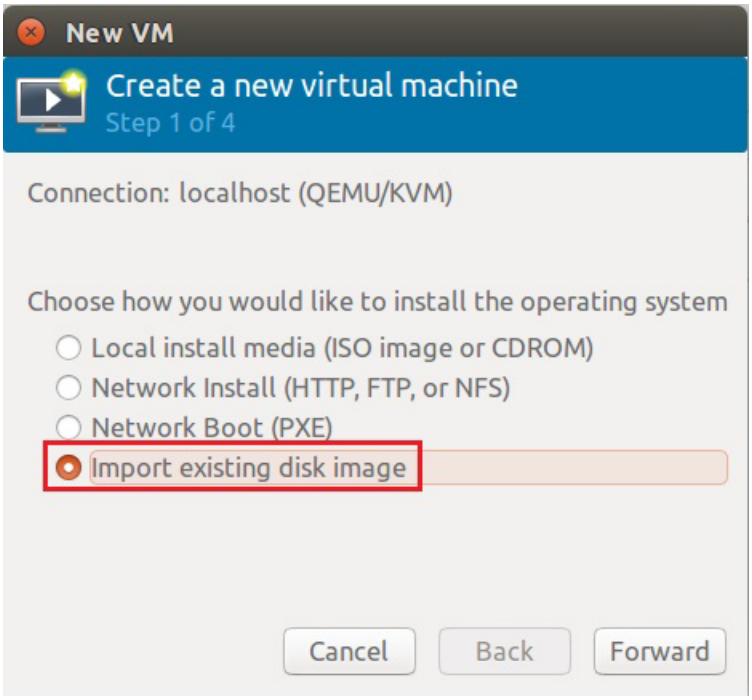
Step 1: Import the FortiADC-VM virtual machine and configure its hardware settings

Before you begin:

- Extract the contents of the FortiADC-VM image .zip file to a folder that you can access from the Virtual Machine Manager.

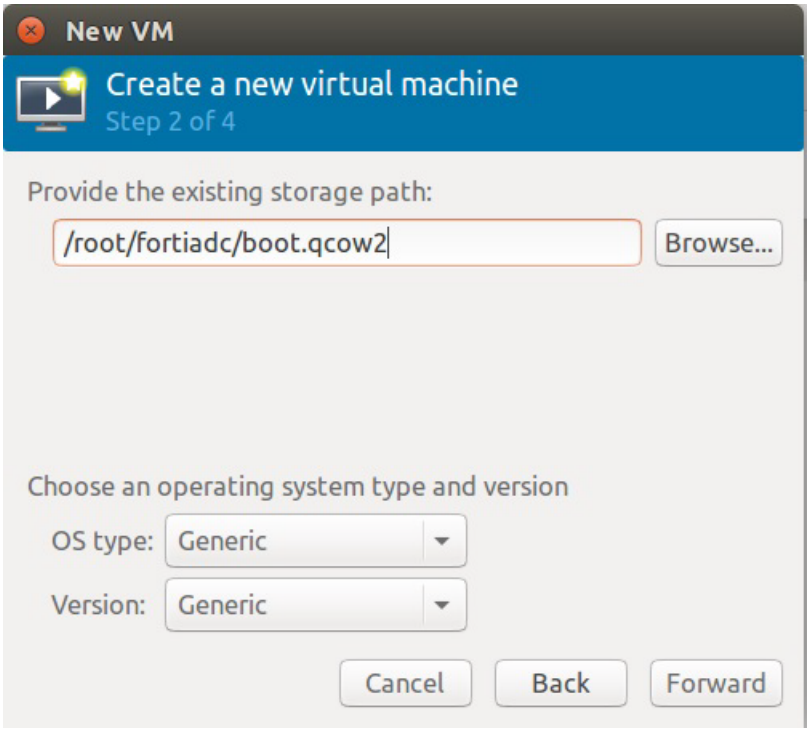
To import the FortiADC-VM virtual machine:

1. On the KVM host server, launch Virtual Machine Manager (virt-manager), and then select **Create a new virtual machine**.
2. Ensure that Connection is localhost (the default value).
3. Select **Import existing disk image**.

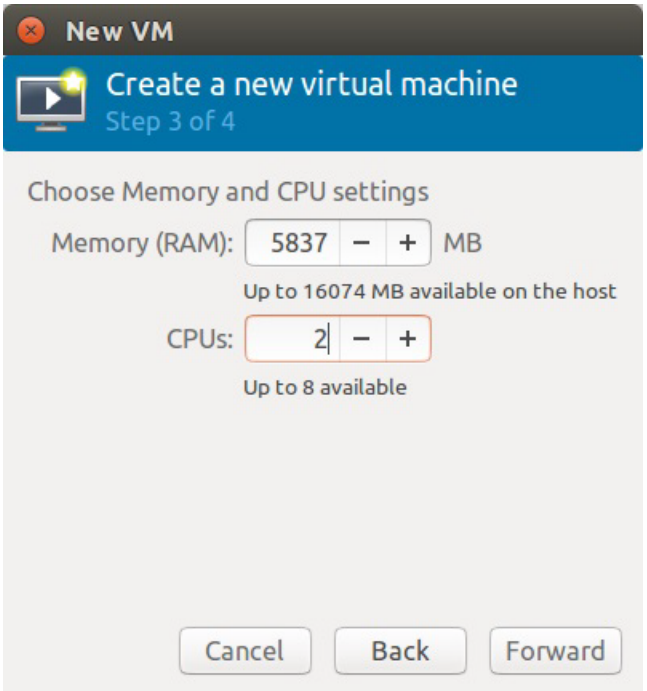


4. Click **Forward**.

5. Click **Browse** to navigate to `boot.qcow2` and select it.
6. Use the default values for **OS Type** and **Version**.

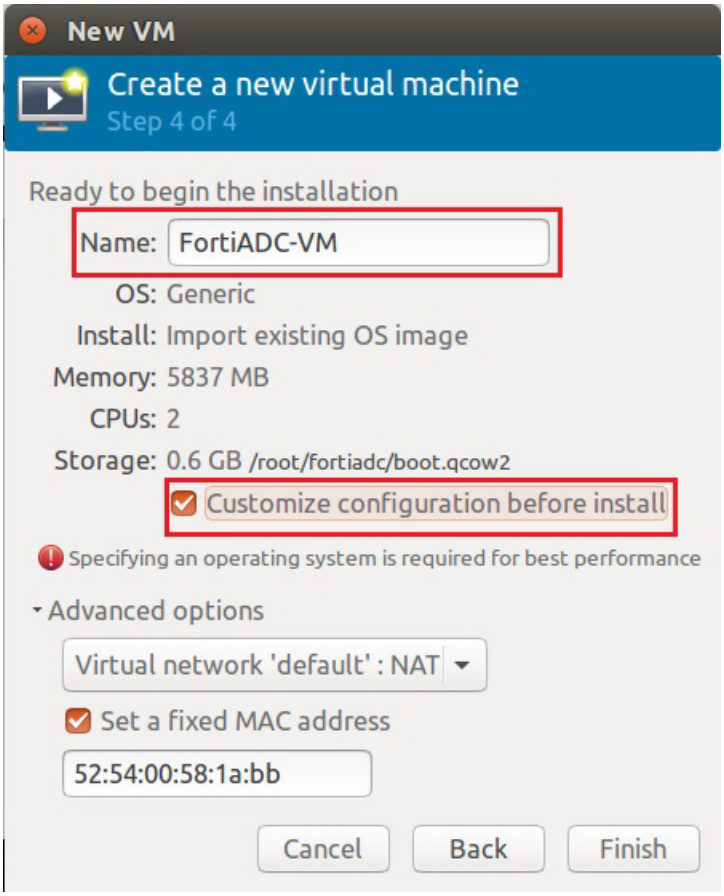


7. Click **Forward**.
8. Specify the amount of memory and number of CPUs to allocate to this virtual machine. Ensure the values do not exceed the maximums for your license.

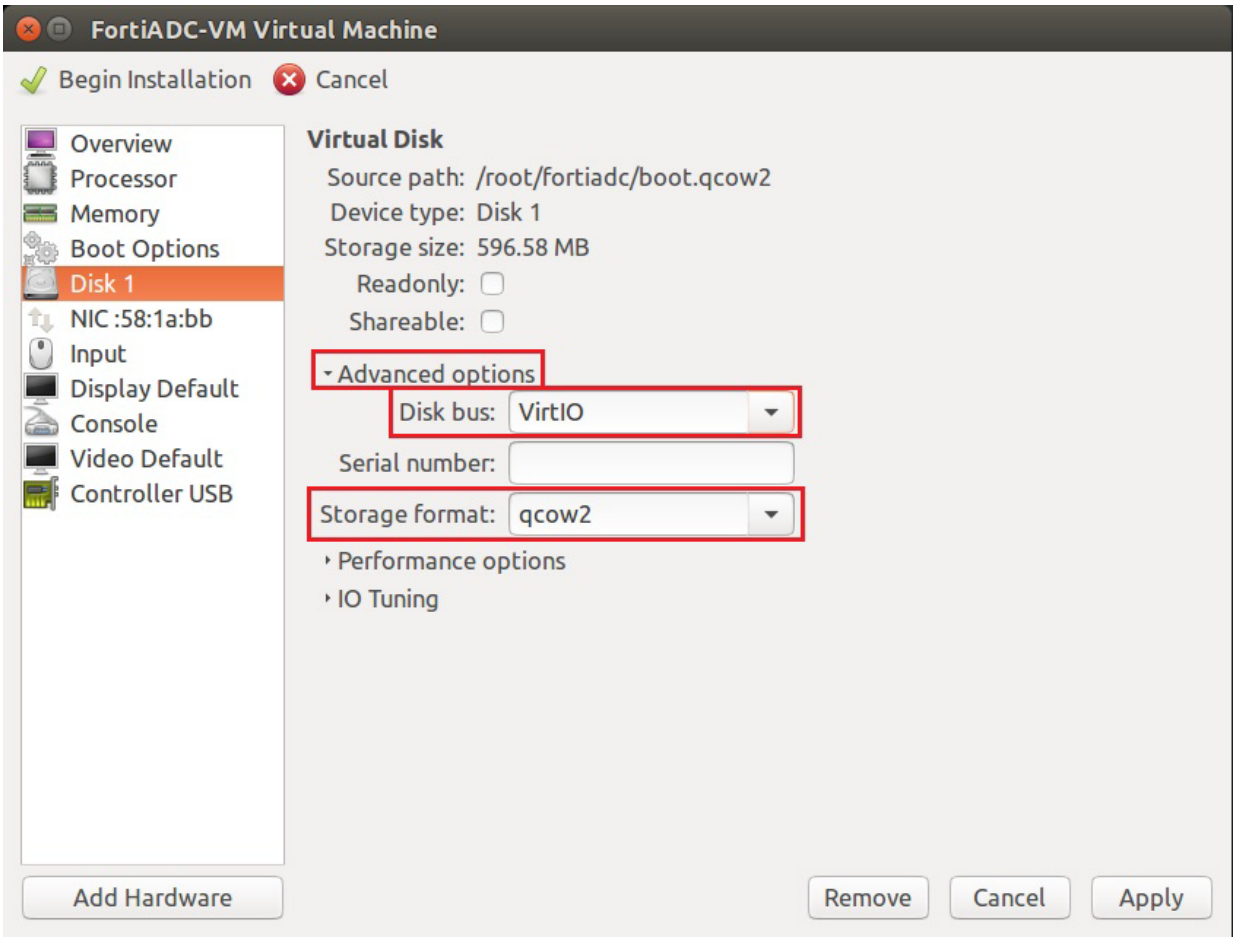


Fortinet recommends that you use at least 4 GB memory.

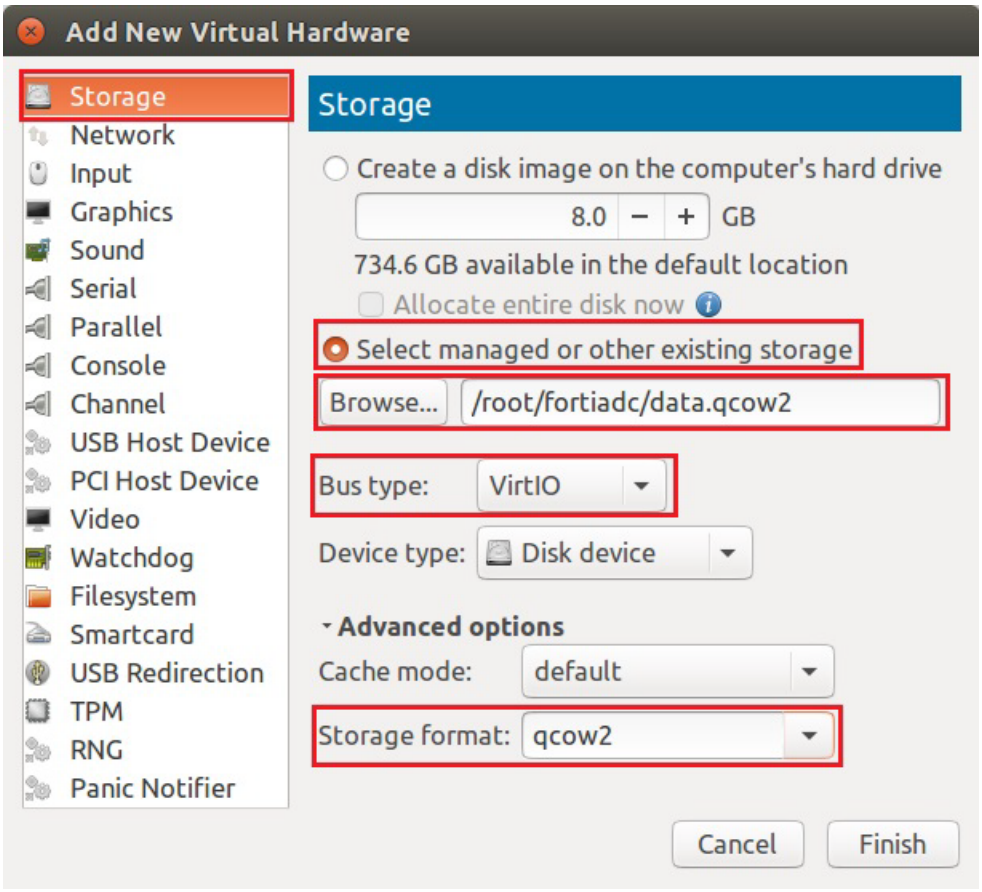
9. Click **Forward**.
10. Enter a name for the VM (for example, `FortiADC-VM`) and select **Customize configuration before install**.



11. Click **Finish**.
12. Select the virtual disk to display its properties.
13. Under Advanced options, for Disk bus, select **Virtio**, and for Storage format, select **qcow2**.

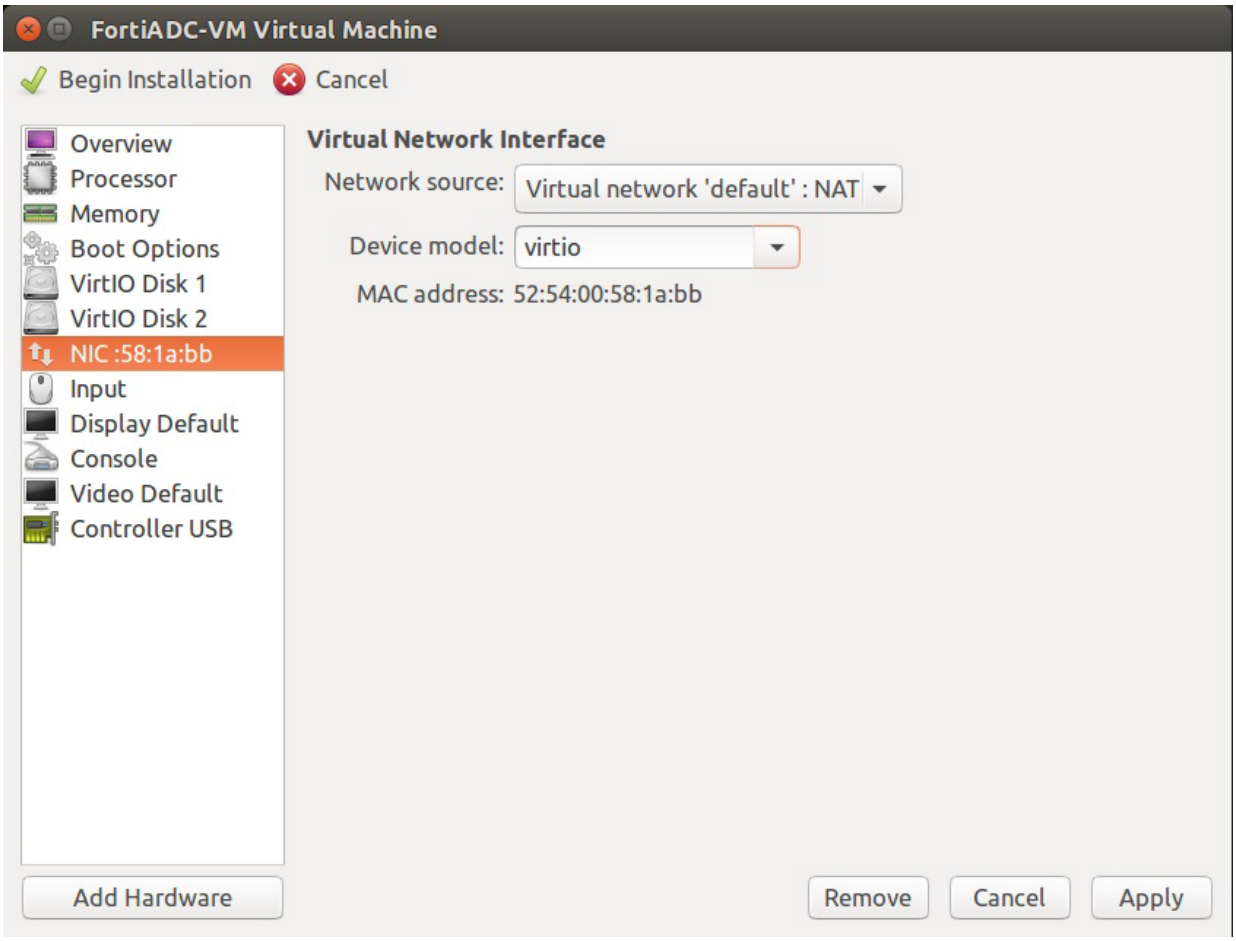


14. Click **Apply**.
15. To add a new virtual storage device, click **Add Hardware**.
16. Do the following:
    - Ensure **Storage** is selected.
    - Select **Select managed or other existing storage**.
    - Click **Browse** to navigate to `data.qcow2` and select it.
    - For Bus type, select **VirtIO**.
    - For Storage format, select **qcow2**.

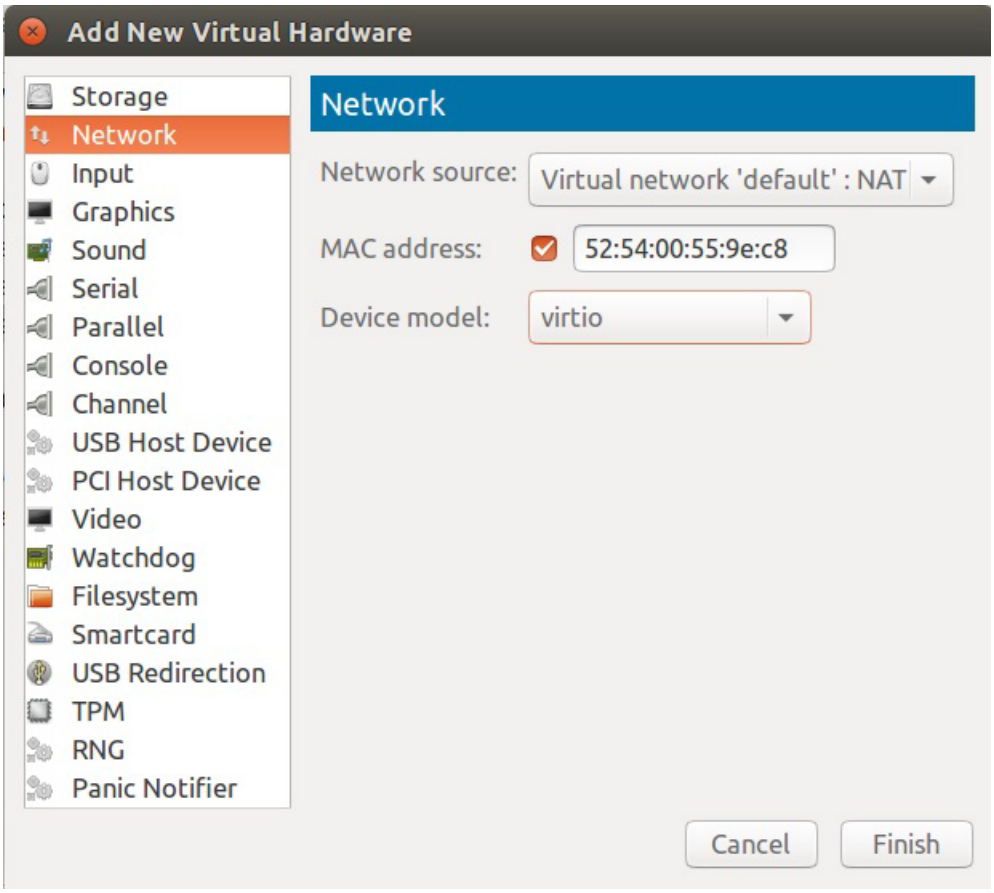


17. Click **Finish**.

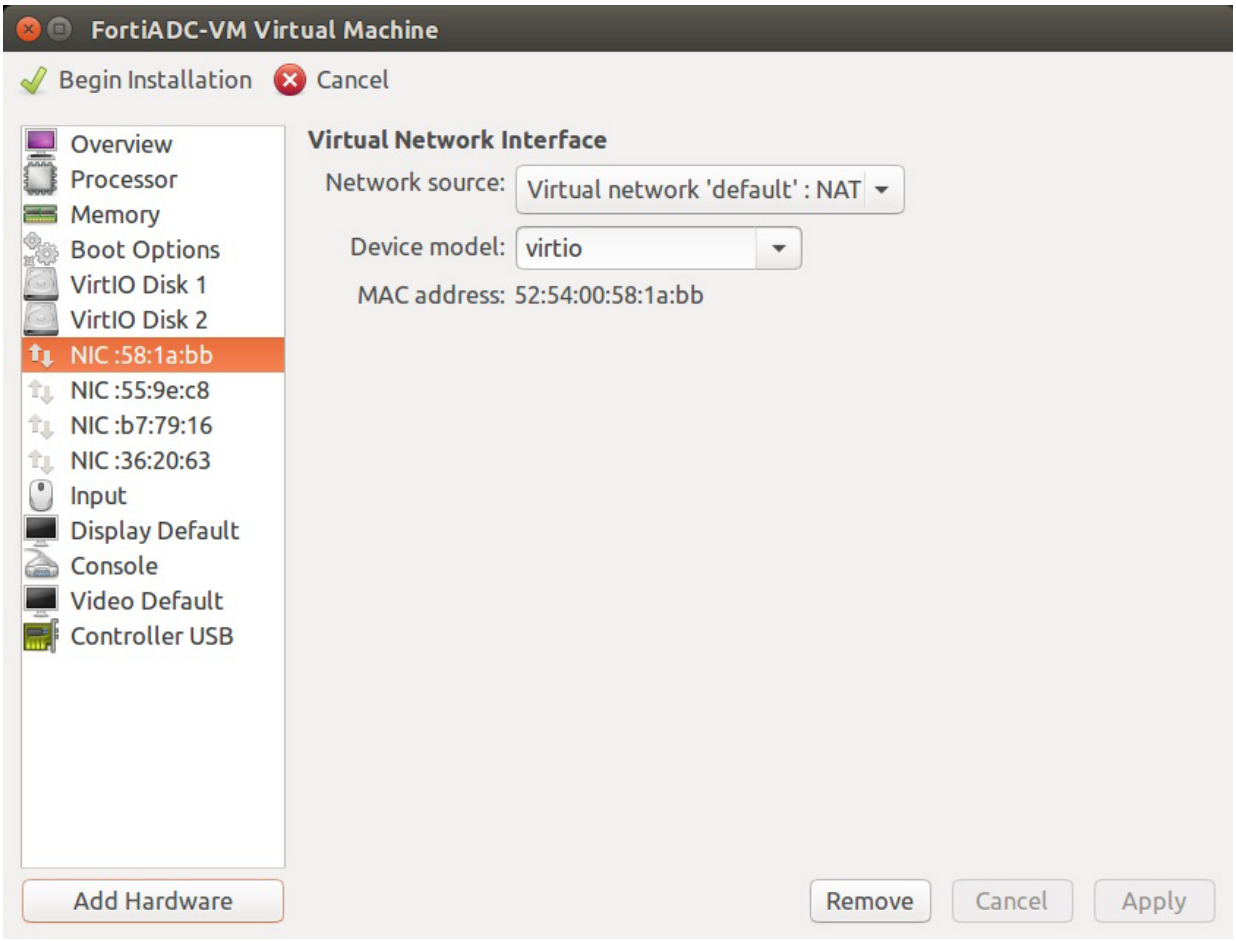
18. Select the virtual network interface (vNIC) and change its type to **virtio**.



19. Click **Apply**.
20. To add an additional vNIC, click **Add Hardware** and then click **Network**.
21. For device model, select **vitrio**.



22. Click **Finish**.
23. Use the vNIC creation steps to add two additional virtio vNICs.



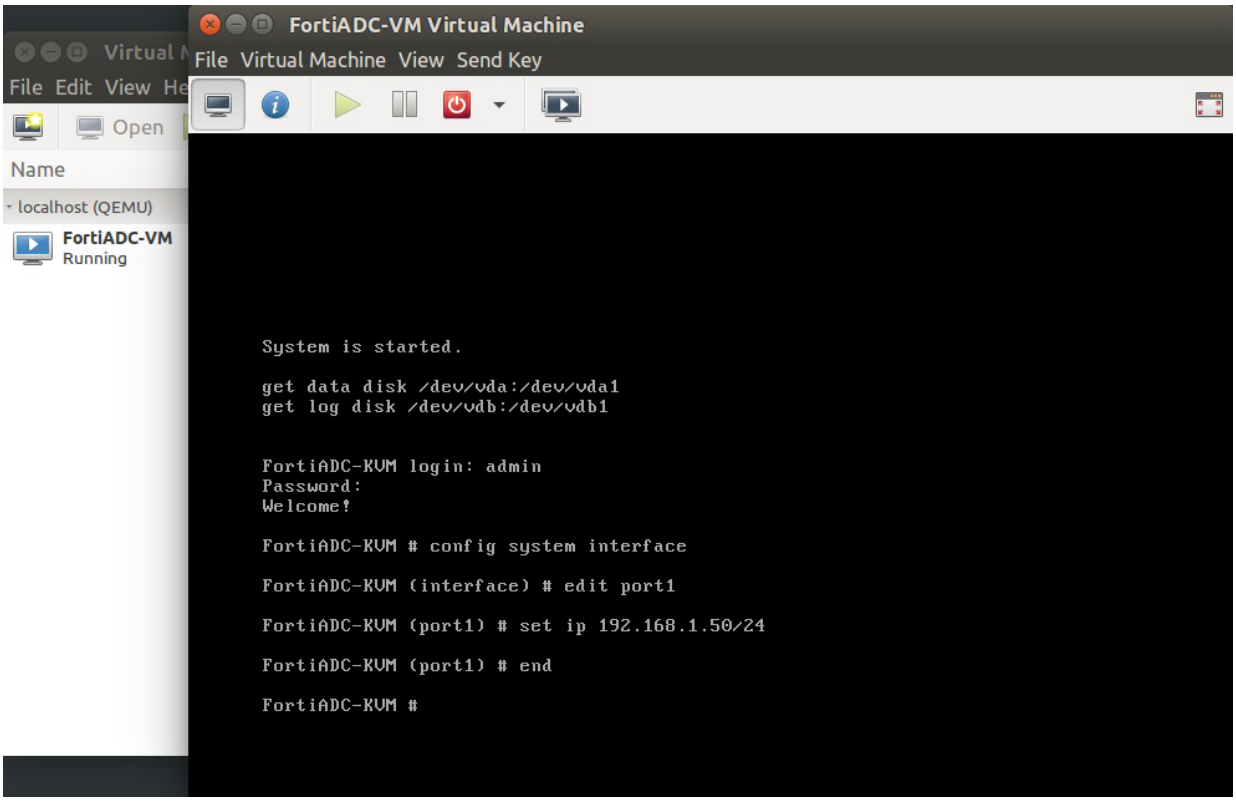
24. Click **Begin Installation**.

Step 2: Configure access to the web UI & CLI

Once it is powered on, you must log in to the FortiADC-VM command-line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. On the KVM host server, launch Virtual Machine Manager (virt-manager).
2. In the pane on the left side, select the name of the virtual appliance, such as FortiADC-VM.
3. Click **Open**. In the window that appears, click the monitor icon.



4. At the login prompt, type `admin` and no password to log in.
5. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit port1
      set ip <address/mask>
      set allowaccess {http https ping snmp ssh telnet}
end
config router static
   edit 1
      set gateway <gateway_address>
end
config system dns
   set primary <dns_address>
   set secondary <dns_address>
end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.
- `<gateway_address>}` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

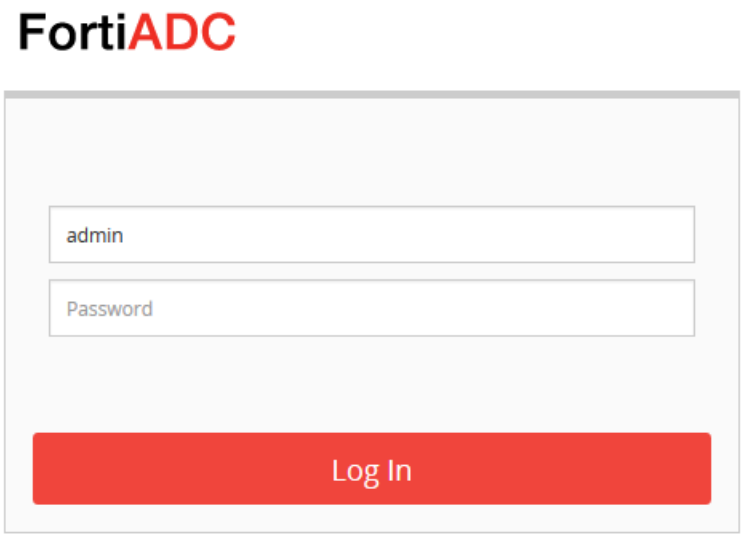
Step 3: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

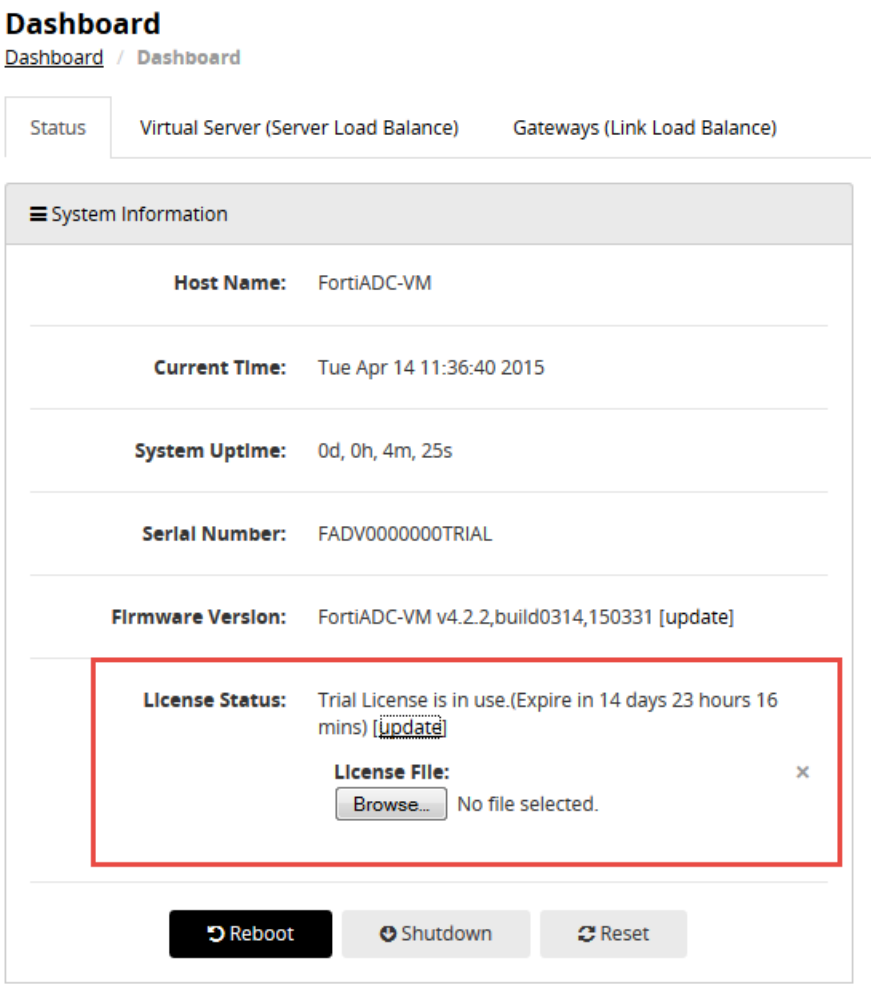
You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as: `https://192.168.1.99/`.
   The web UI login page appears.



3. Use the username `admin` and no password to log in.
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The web UI opens to the dashboard.
5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

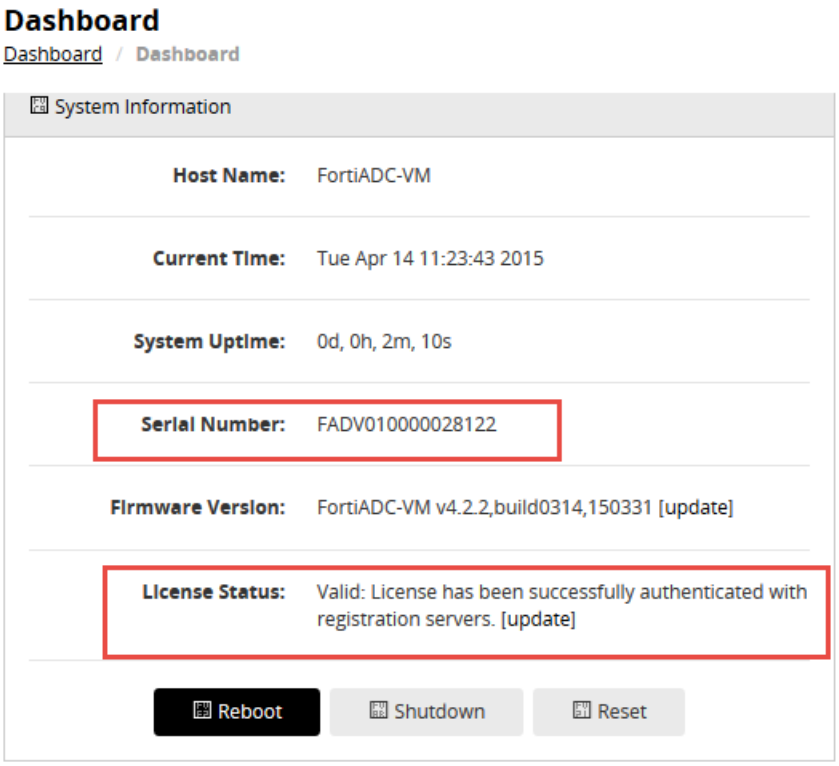


After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```



If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
```

```
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

What's next?

At this point, the FortiADC virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the *FortiADC Handbook* for information on getting started with feature configuration.

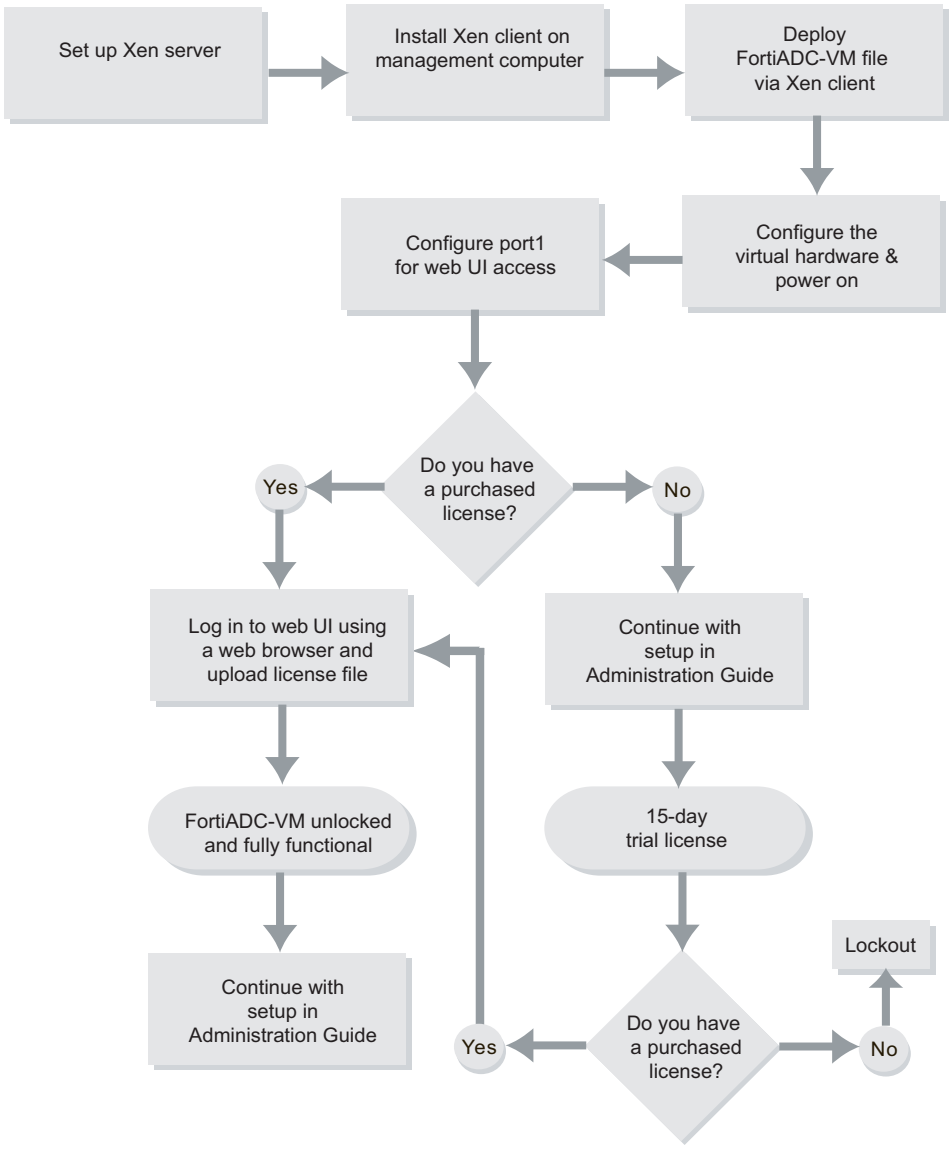
Chapter 5: Deploying FortiADC-VM on Citrix Xen

This chapter provides procedures for deploying FortiADC-VM on Citrix Xen. It includes the following information:

Installation overview

The diagram below overviews the process for installing FortiADC-VM on Citrix XenServer, which is described in the subsequent text.

Basic steps for installing FortiADC-VM (Citrix XenServer)

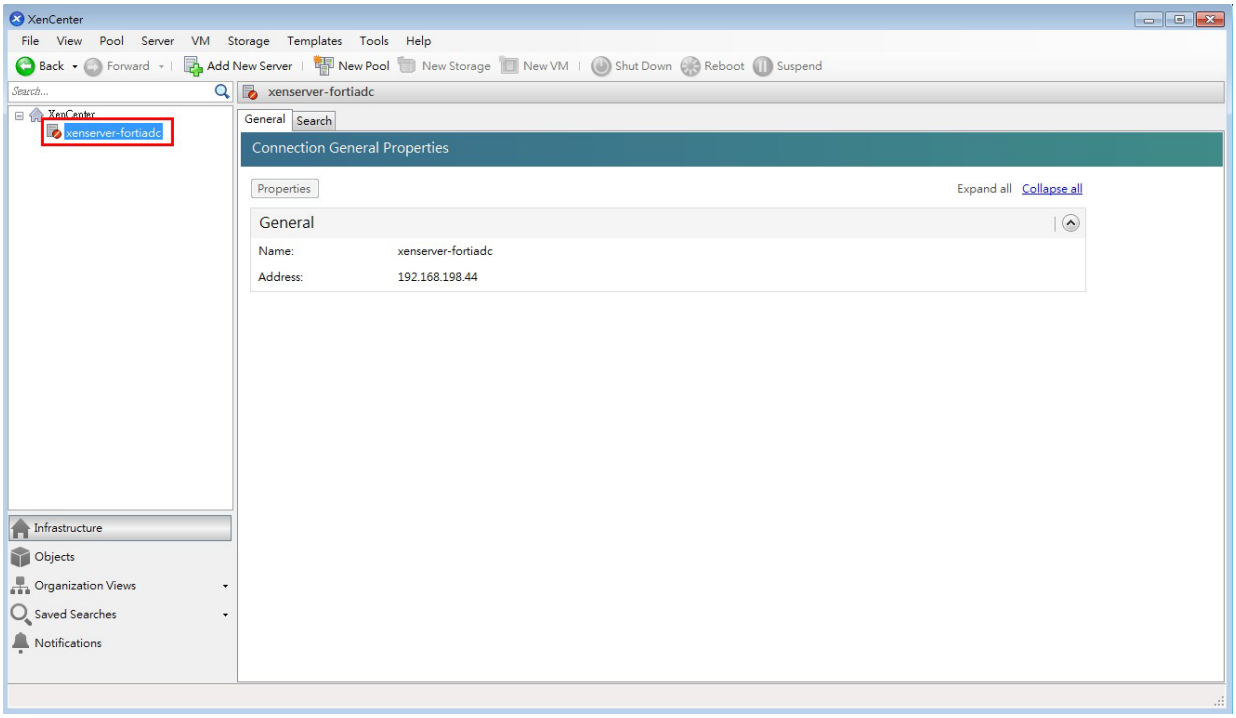


Step 1: Deploy the OVF file

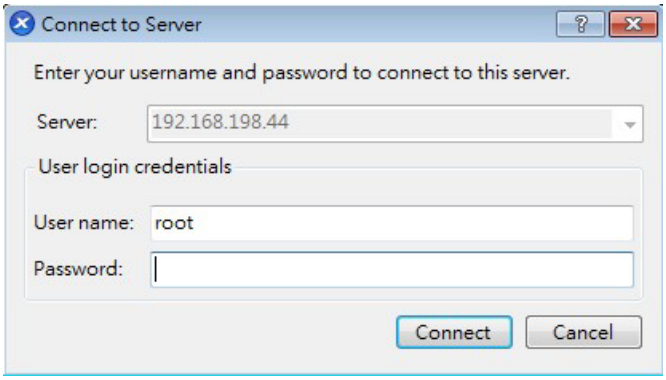
You must first use Citrix XenCenter to convert the open virtualization format (OVF) package to a format that can be used with Citrix XenServer, and to deploy the **fortiadc-vm-xen.ovf** template package.

To deploy the virtual appliance:

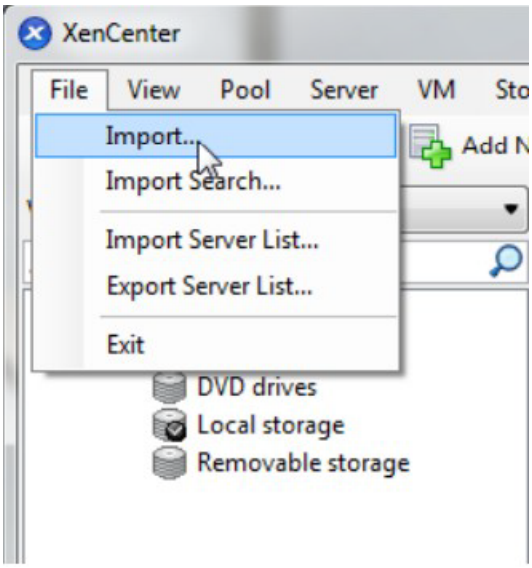
1. On your management computer, start Citrix XenCenter.



2. In the pane on the left side, double-click the name of the XenServer to display the authentication dialog.

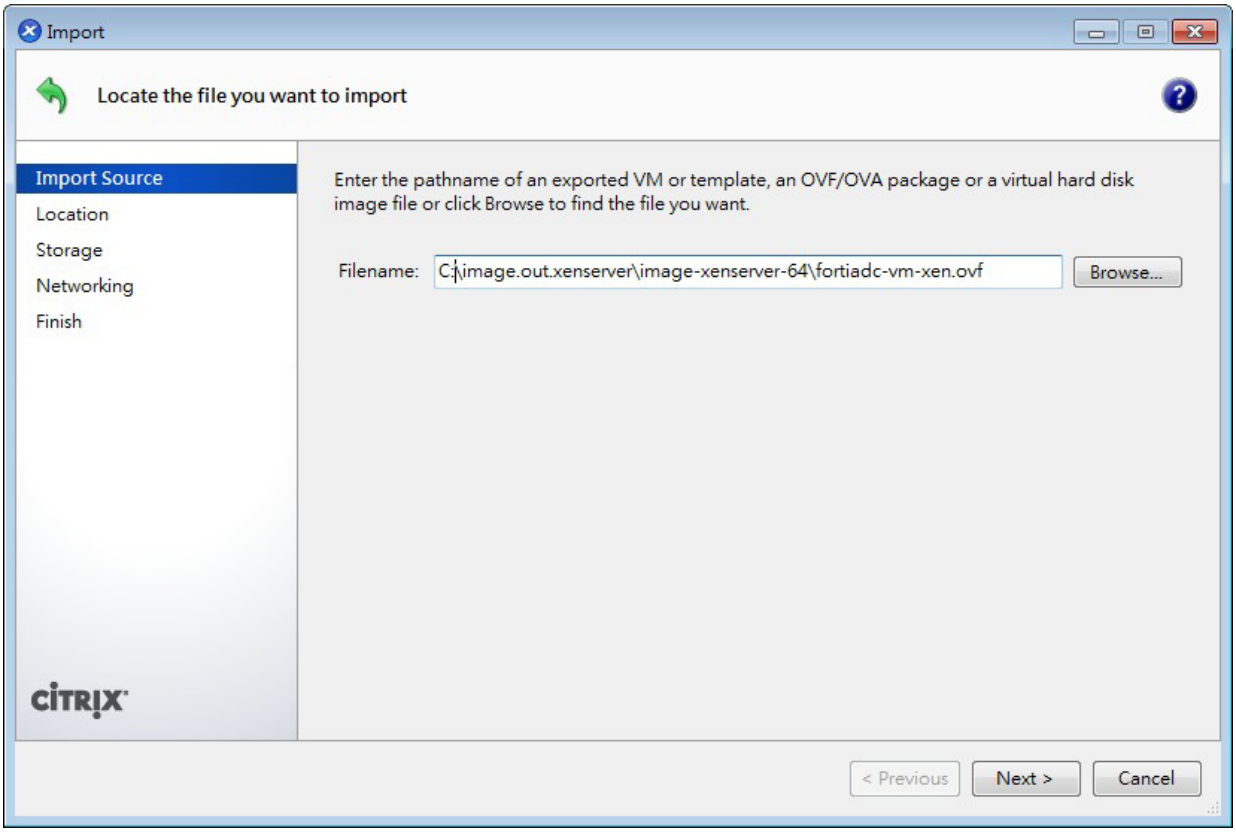


3. Specify the Citrix XenServer server IP address or FQDN, username, and password to log in.
4. Go to **File > Import**.

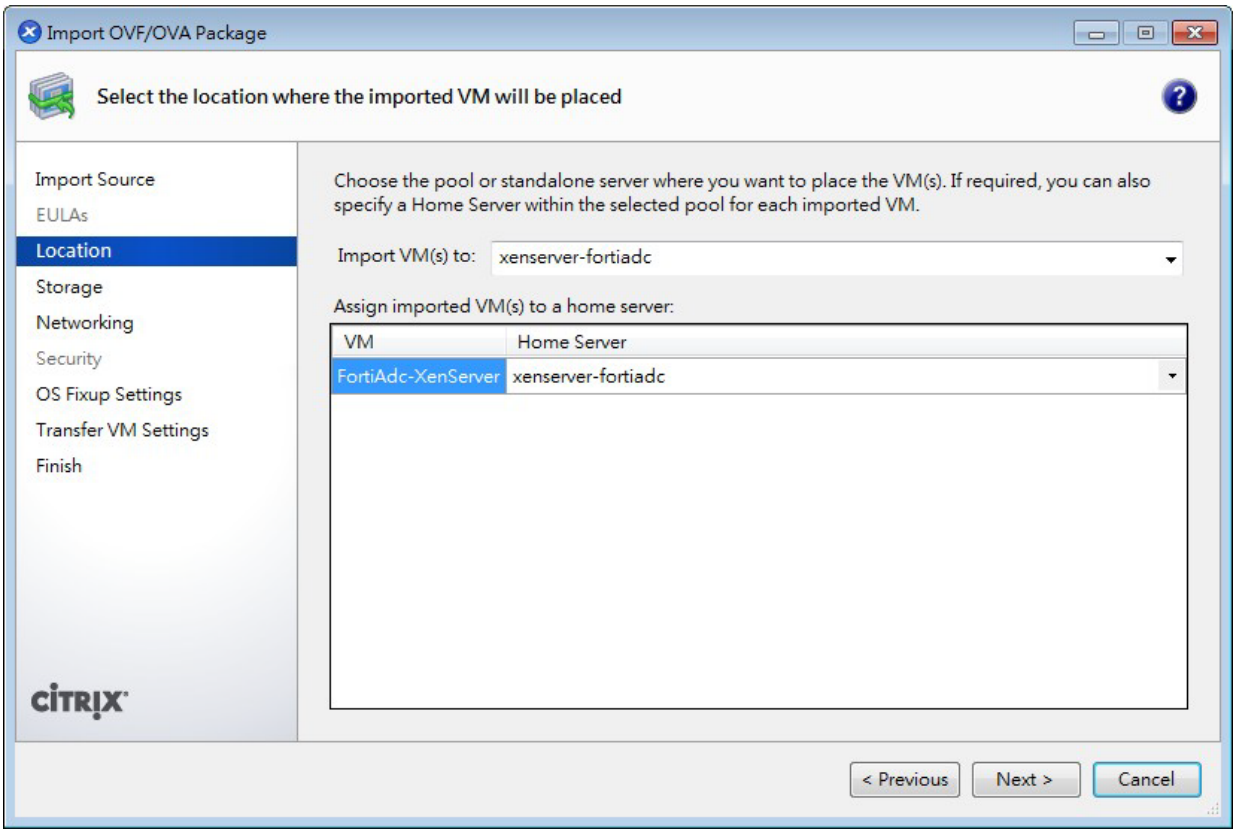


An import wizard will appear.

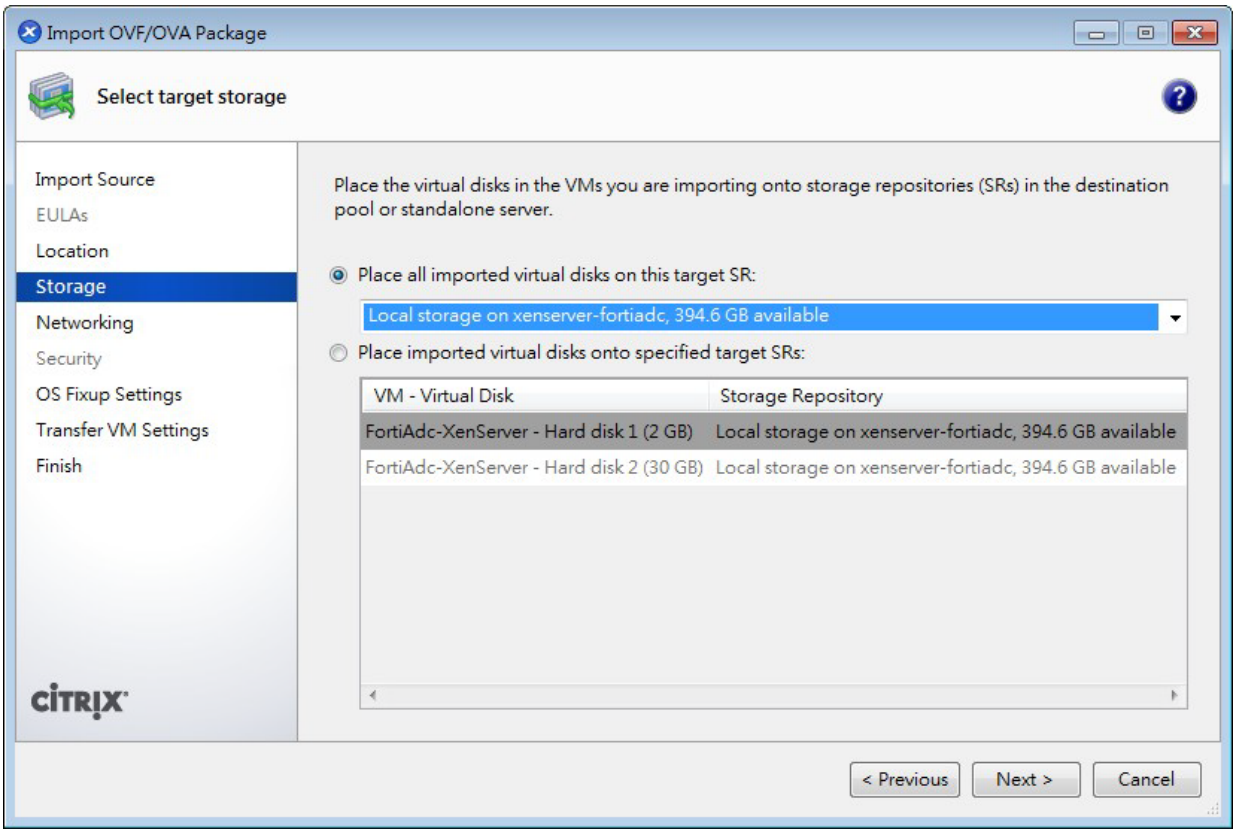
5. Click the **Browse** button to select the f**ortiadc-vm-xen.ovf** template package, then click **Next**.



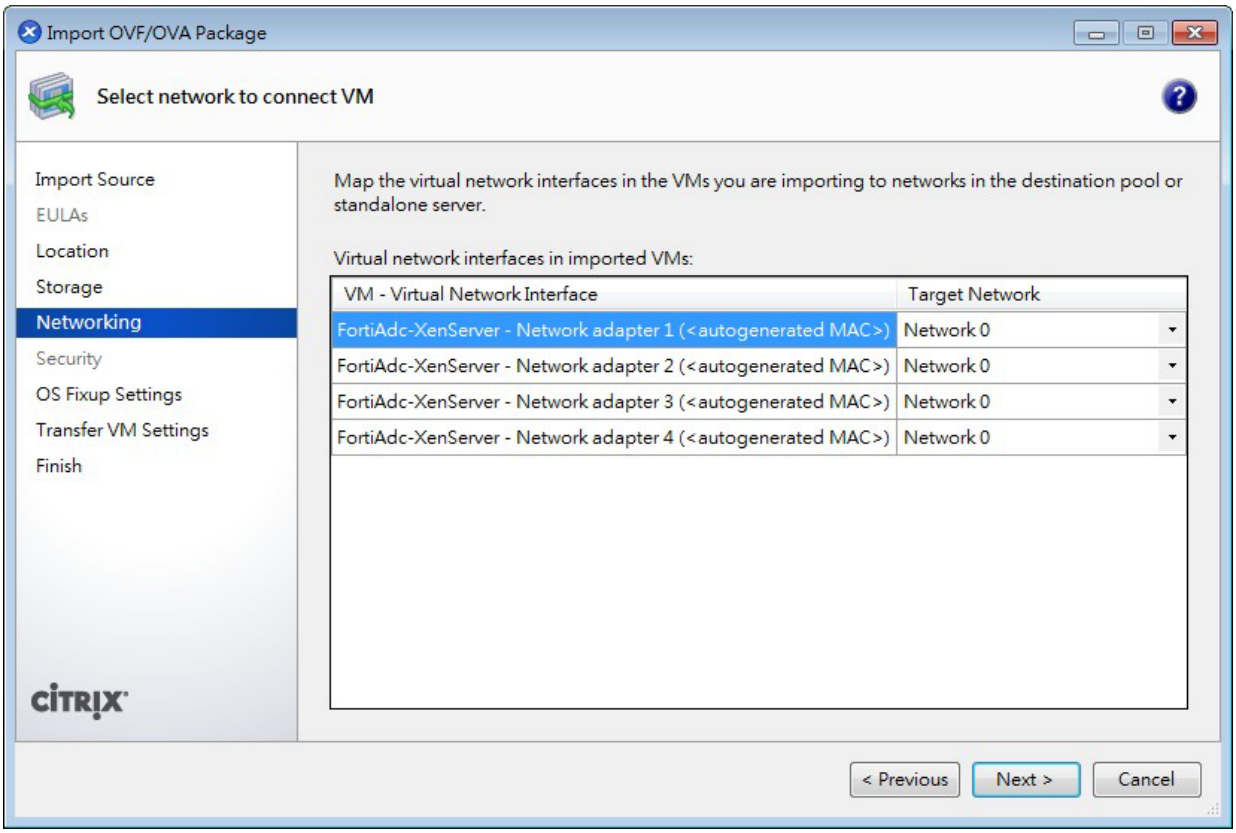
6. Confirm the XenServer where you want to deploy FortiADC-VM, then click **Next**.



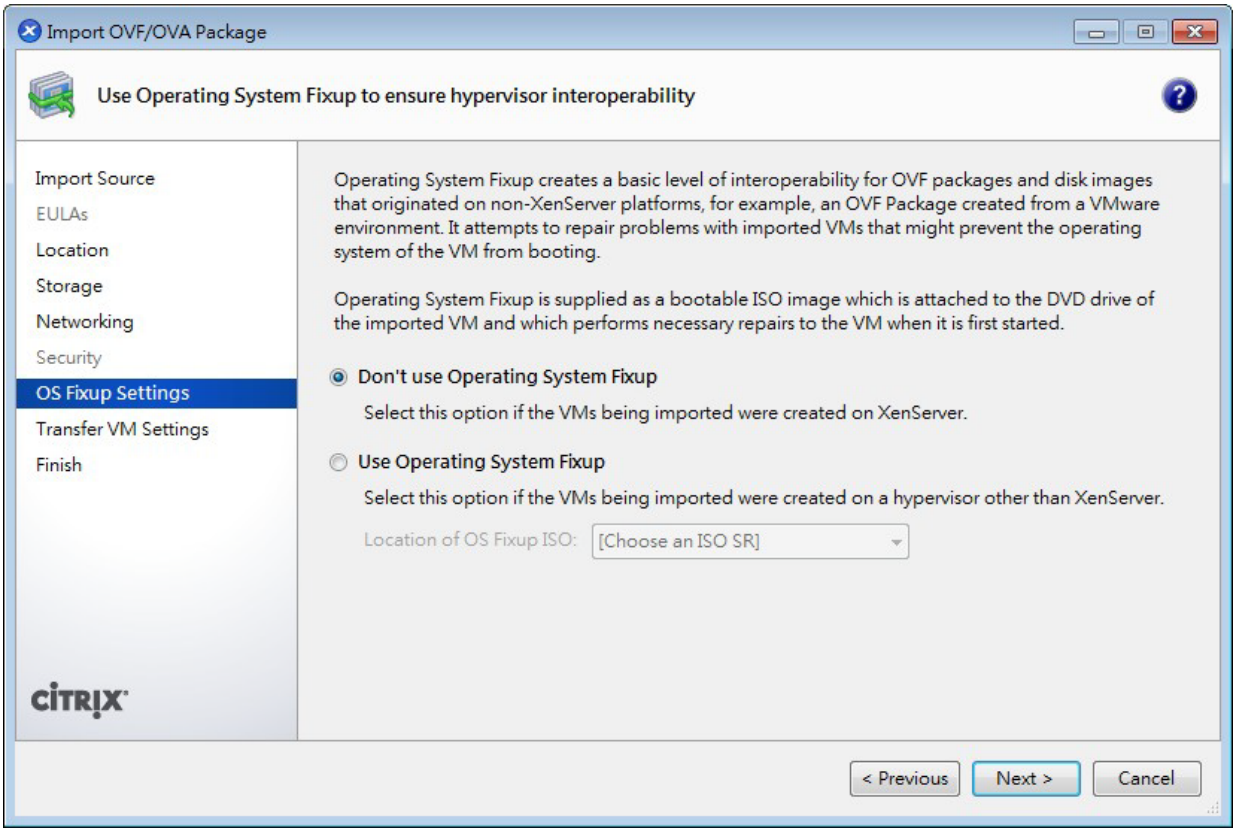
7. If you have multiple storage repositories, such as if you have an NFS or Windows (CIFS) share, select where the vDisks will be physically stored, then click **Next**.



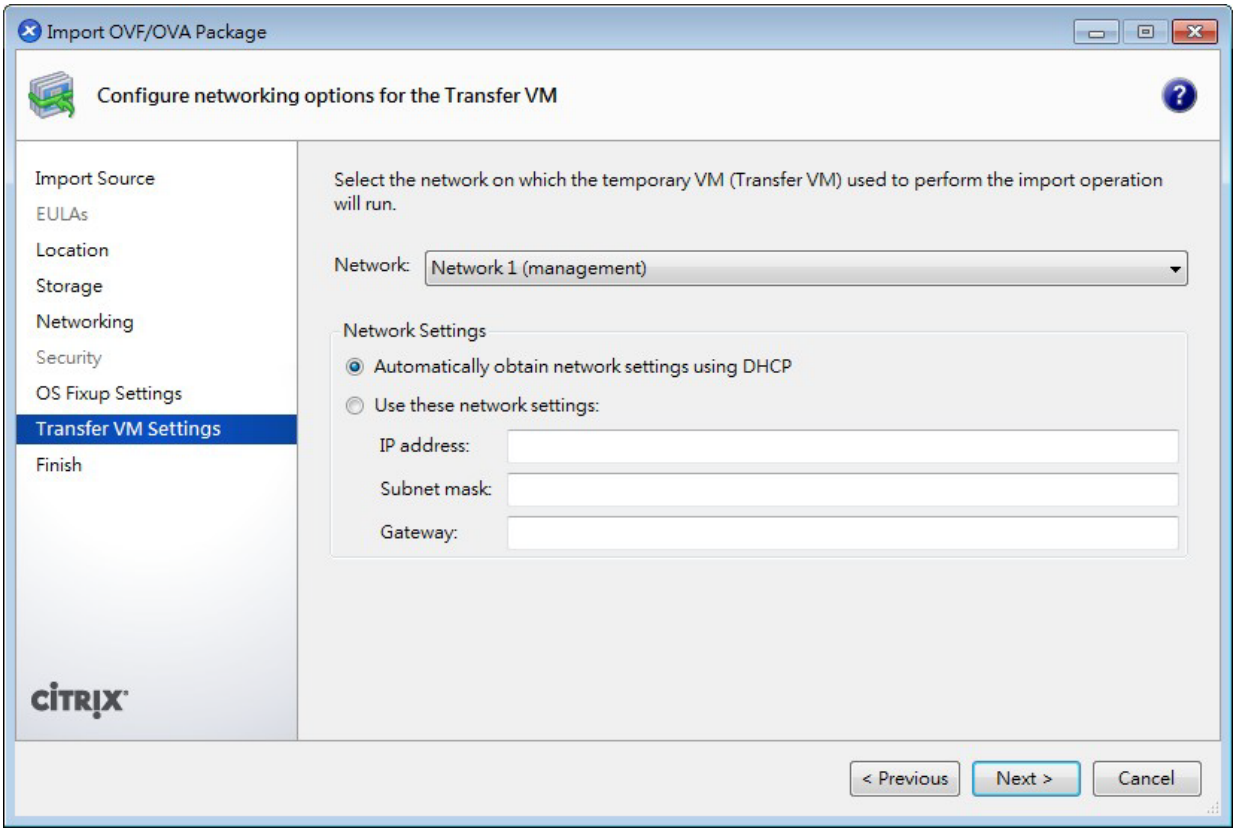
8. Configure how each vNIC (virtual network adapter) in FortiADC-VM will be mapped to each vNetwork on that XenServer, then click **Next**.



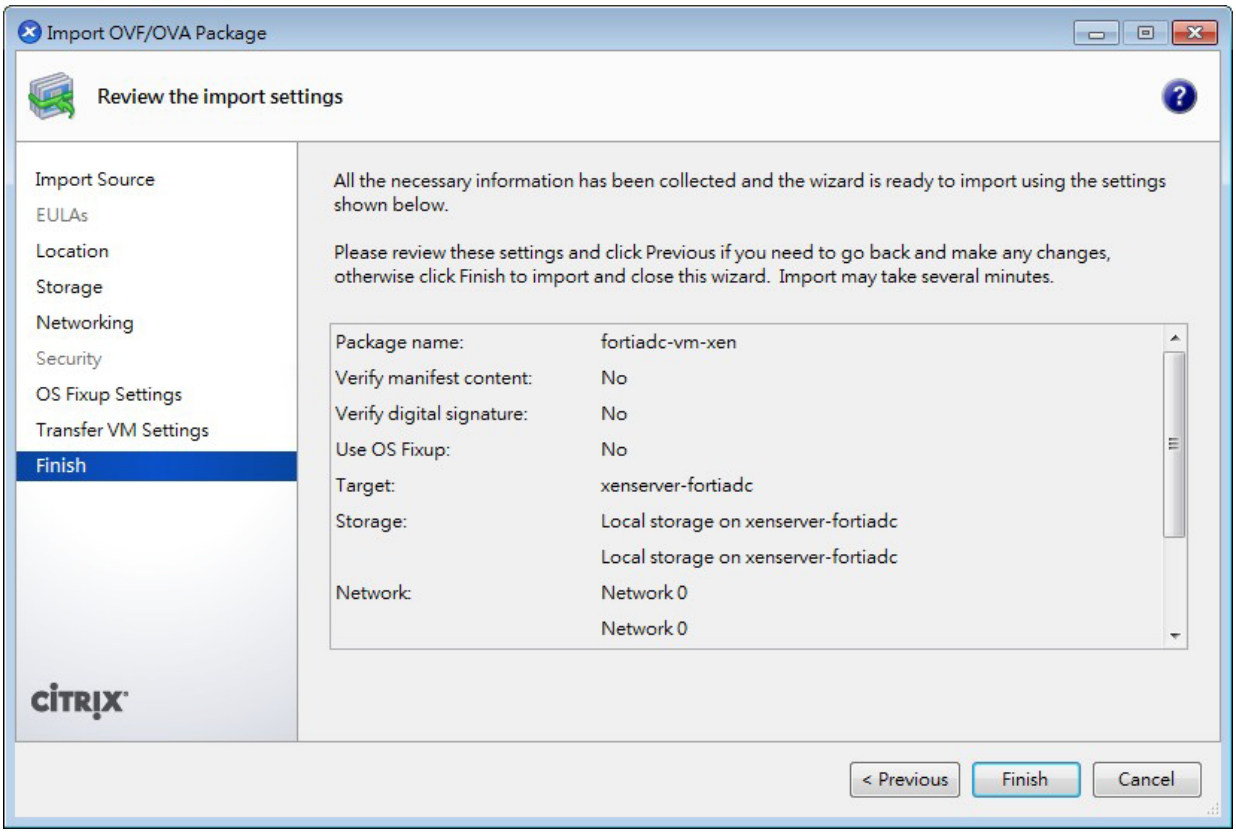
9. Click **Next** to skip OS fixup.



10. Configure temporary network settings that XenServer can use to download FortiADC-VM, then click **Next**.



11. Click **Finish** to send the FortiADC-VM image and its VM settings to XenServer.



When complete, the deployment appears in the list of deployed VMs for that XenServer, in the pane on the left side of XenCenter.

Do not power on the virtual appliance until you have completed the following steps:

- Resize the virtual disk (VMDK).
- Set the number of vCPUs.
- Set the vRAM on the virtual appliance.
- Map the virtual network adapter(s).

These settings must be configured in the VM environment, not the FortiADC OS.

Step 2: Configure virtual hardware settings

After installing the FortiADC-VM image and before powering on the virtual appliance, log into Citrix XenServer and configure the virtual appliance hardware settings to suit the size of your deployment.

Table 5 summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Table 5: Virtual hardware settings

Component	Default	Guidelines
Hard drive	32 GB	32 GB is insufficient for most deployments. You must upgrade the hard drive before you power on the appliance. After you power on the appliance, you must reformat the FortiADC OS log disk with the following command: `execute formatlogdisk`
CPU	1 CPU	1 CPU is appropriate for a VM01 license. Upgrade to 2, 4, or 8 CPU for VM02, VM04, and VMO8 licenses, respectively.
RAM	4 GB	2 GB is the minimum. 4 GB is recommended.
Network interfaces	Bridging vNICs are mapped to a port group on one virtual switch (vSwitch). In versions below 5.2, 3 vNICs are mapped; in version 5.2 and later, 7 vNICs are mapped.	Change the mapping as required for your VM environment and network.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk before powering on.

This step is not applicable if the virtual appliance will use external network file system (such as NFS) datastores.

The FortiADC-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. **Resize the vDisk before powering on the virtual machine.**

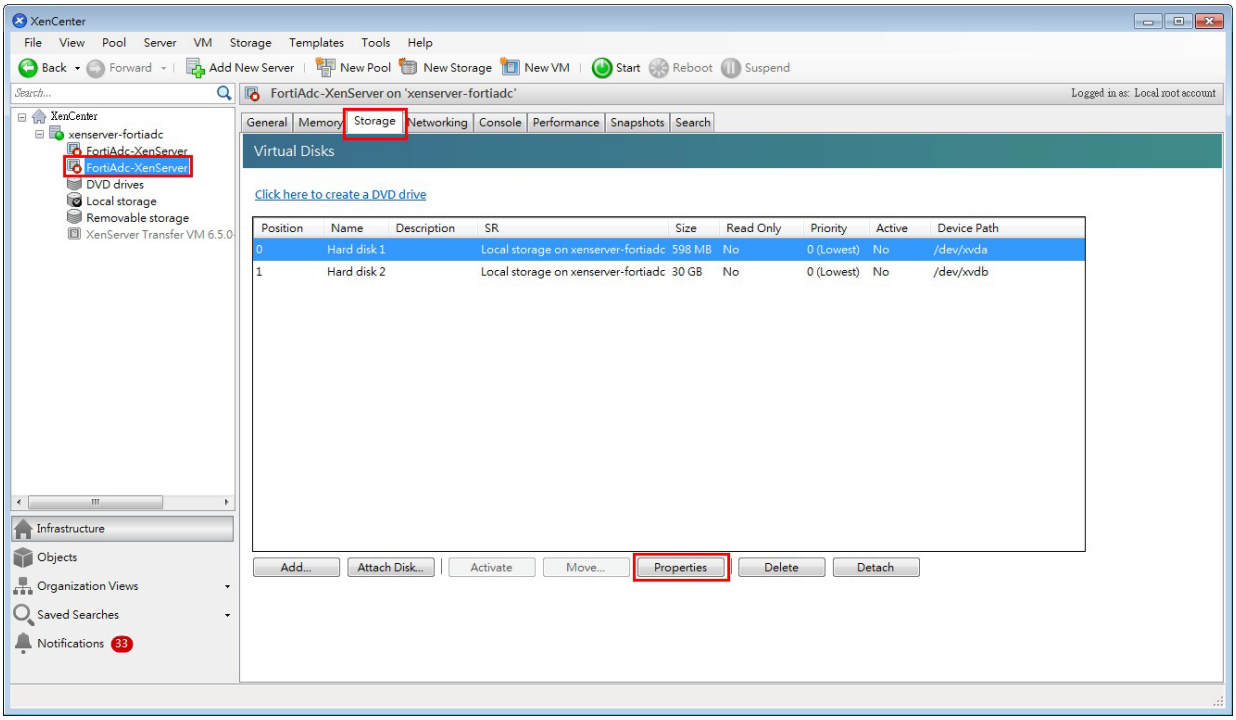
Before doing so, make sure that you understand the effects of your vDisk settings.

For example, if you have an 800 GB data store which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiADC-VM.

Consider also that, depending on the size of your network, you might require more or less storage.

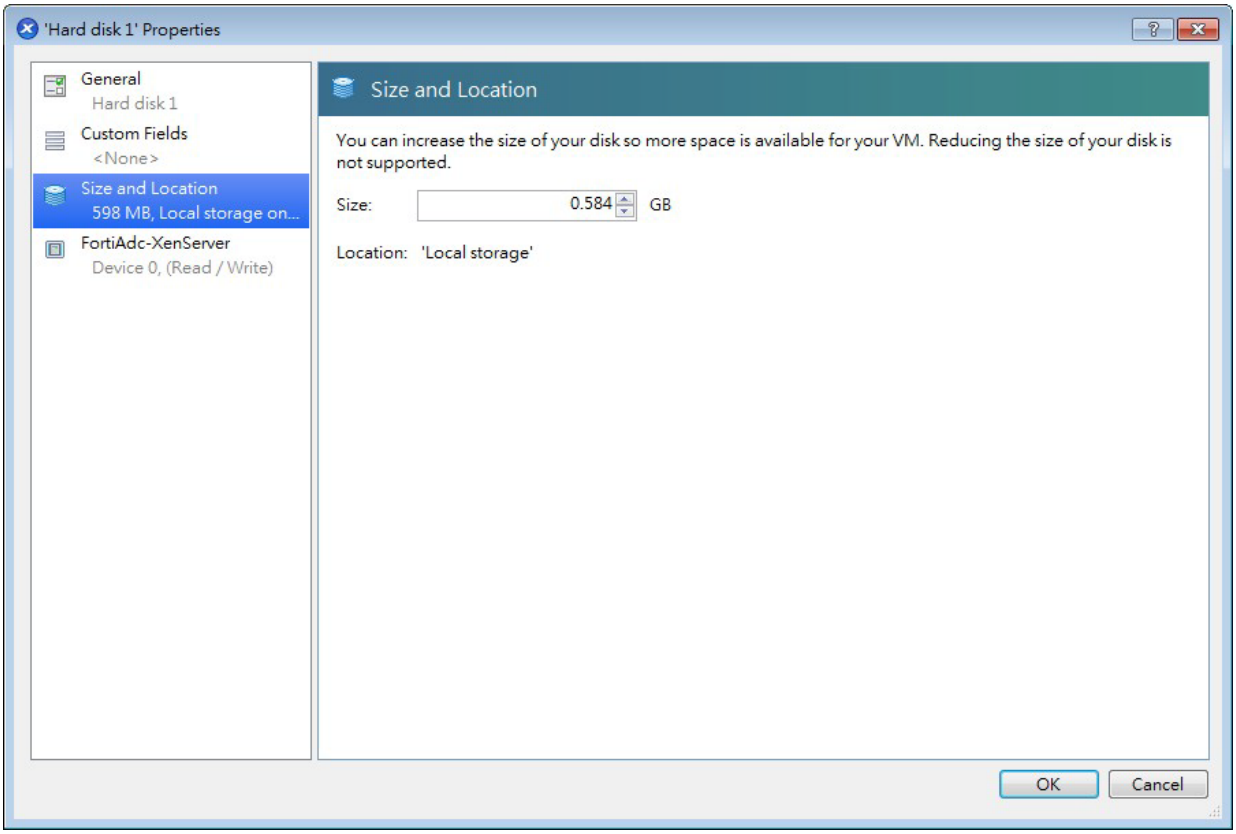
To resize the vDisk:

1. Log into Citrix XenCenter server.
2. In the pane on the left side, select the name of the FortiADC-VM instance on that server. The pane on the right side will change to show the settings for this specific virtual machine.



3. In the pane on the right side, click the **Storage** tab, then click the **Properties** button.

4. Adjust the maximum size of the vDisk, then click **OK**.

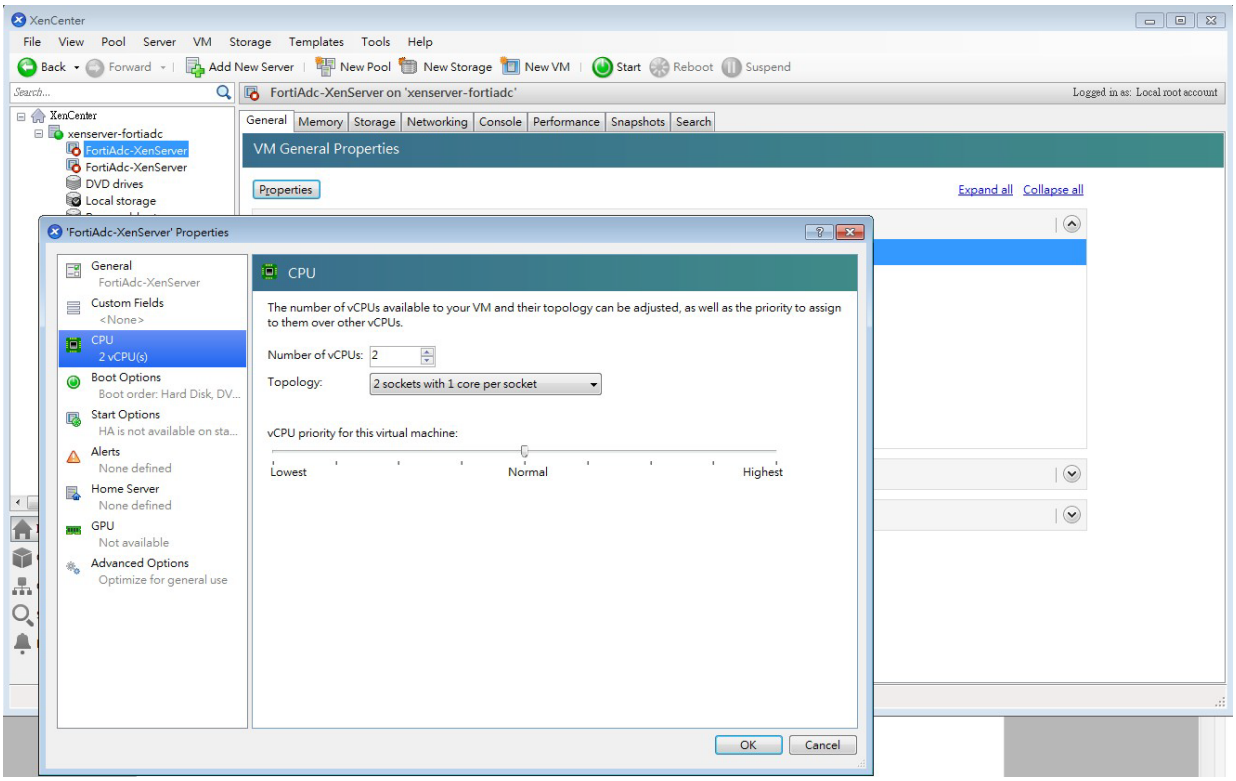


Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiADC-VM license that you purchased, you can allocate up to 1, 2, 4, or 8 vCPUs.

To change the number of vCPUs:

1. Log into Citrix XenCenter server.
2. In the pane on the left side, select the name of the FortiADC-VM instance.
   The pane on the right side will change to show the settings for this specific virtual machine.
3. In the pane on the right side, click **Properties**.
   The virtual appliance's properties dialog appears.
4. In Number of VCPUs, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



5. Click **OK.**

Configuring the virtual RAM (vRAM) limit

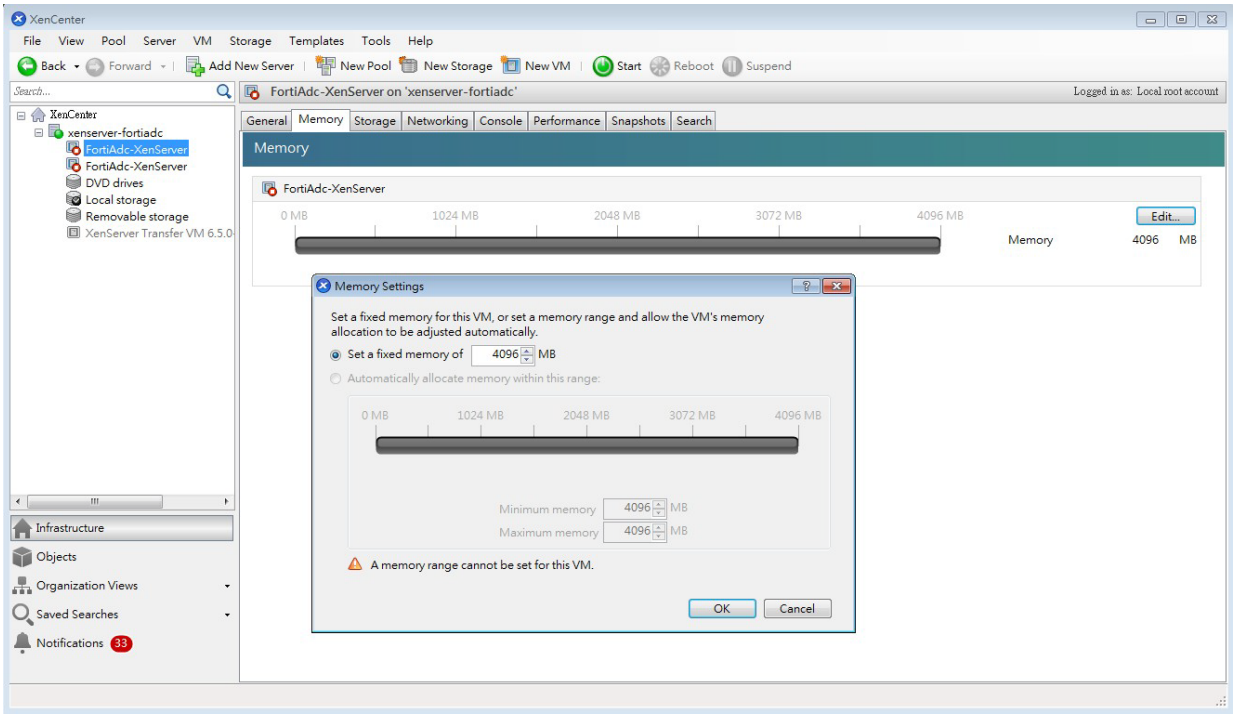
FortiADC-VM comes pre-configured to use 4 GB of vRAM. You can change this value.

We recommend at least 4 GB RAM.

To change the amount of vRAM

1. Log into the Citrix XenServer.
2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In the pane on the left side, select the name of the FortiADC-VM instance on that server.
   The pane on the right side will change to show the settings for this specific virtual machine.
4. In the pane on the right side, click the **Memory** tab, then click **Edit**.
   The virtual appliance's memory settings dialog appears.

5. Adjust the maximum amount in gigabytes (GB) of the vRAM to allocate, then click **OK**.



Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiADC-VM network adapter ports to the host computer physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and don't need to be changed.

If you are unsure of your network mappings, try bridging first **before** non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs and the transparent modes.

When you deploy the FortiADC-VM package, 10 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 10 network interfaces in FortiADC-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if either your VM environment requires it.

The following table provides an example of how vNICs could be mapped to the physical network ports on a server.

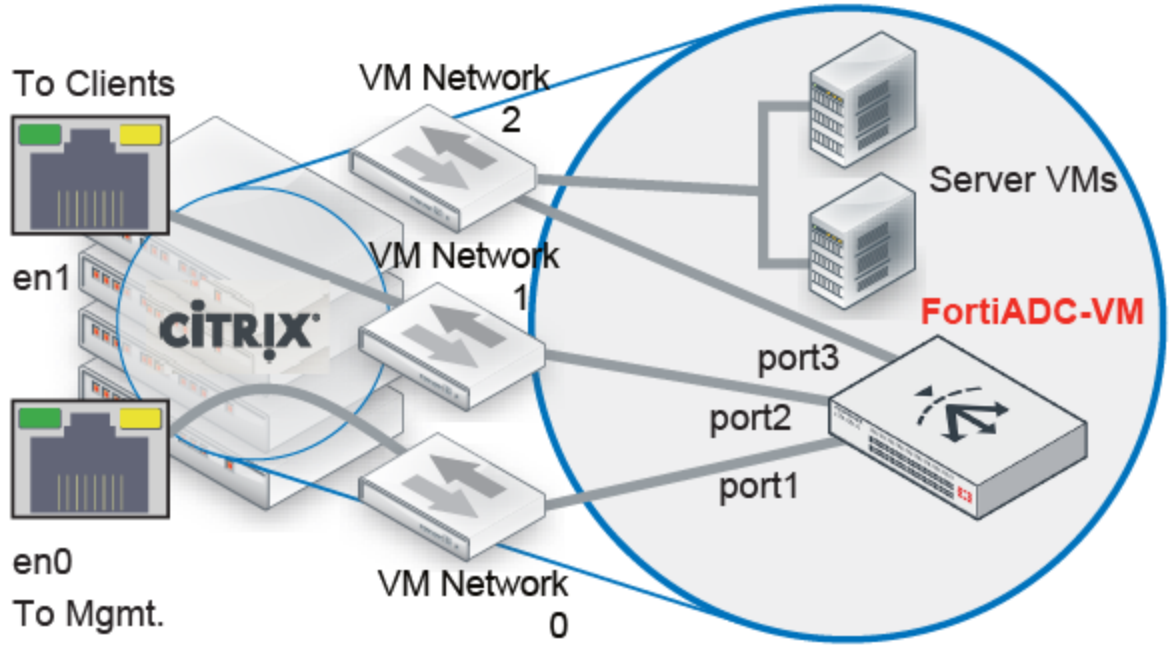
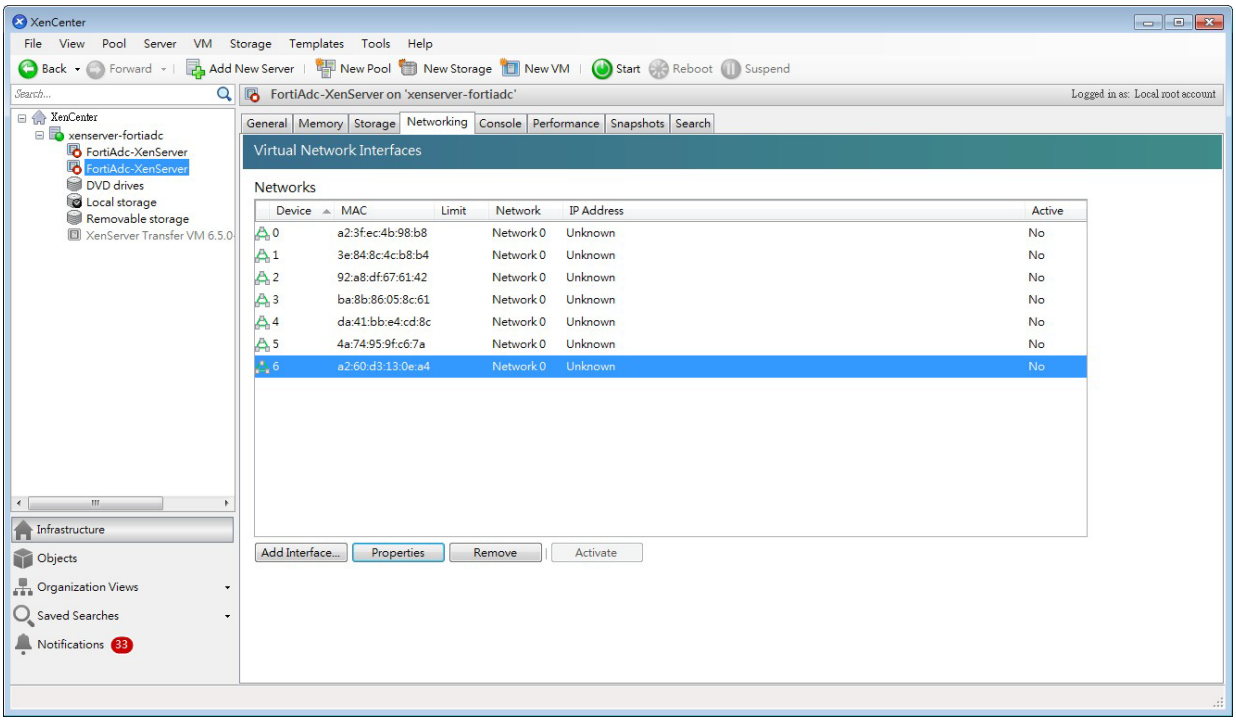


Table 6: Example: Network mapping

Citrix XenServer			FortiADC-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiADC-VM	Network Interface Name in Web UI/CLI
eth0	Network 0	Management	port1
eth1	Network 1	External	port2
	Network 2	Internal	port3

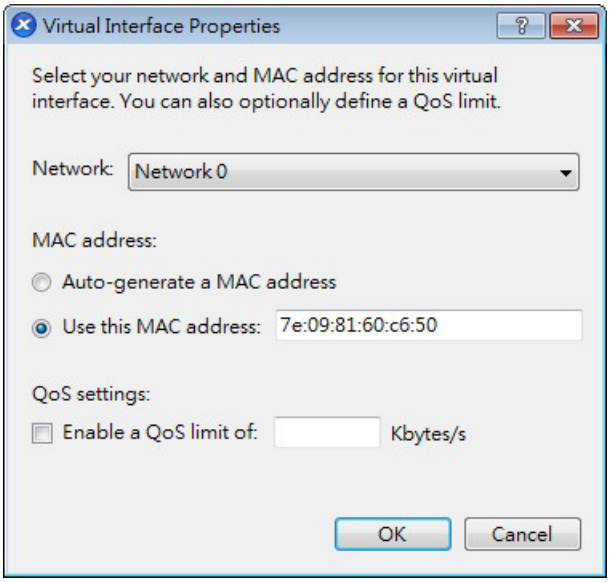
To map network adapters:

1. Log into the Citrix XenServer.
2. In the pane on the right side, click the **Networking** tab.



3. Click the name of a virtual network adapter to display its settings.
4. From the **Network** drop-down list, select the virtual network mapping for the virtual network adapter.

   The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC is mapped to the virtual network (vNetwork) named **Network 0.**



5. Click **OK**.

Step 3: Power on the virtual appliance

After the virtual appliance software has been deployed and its virtual hardware configured, you can power on the virtual appliance.

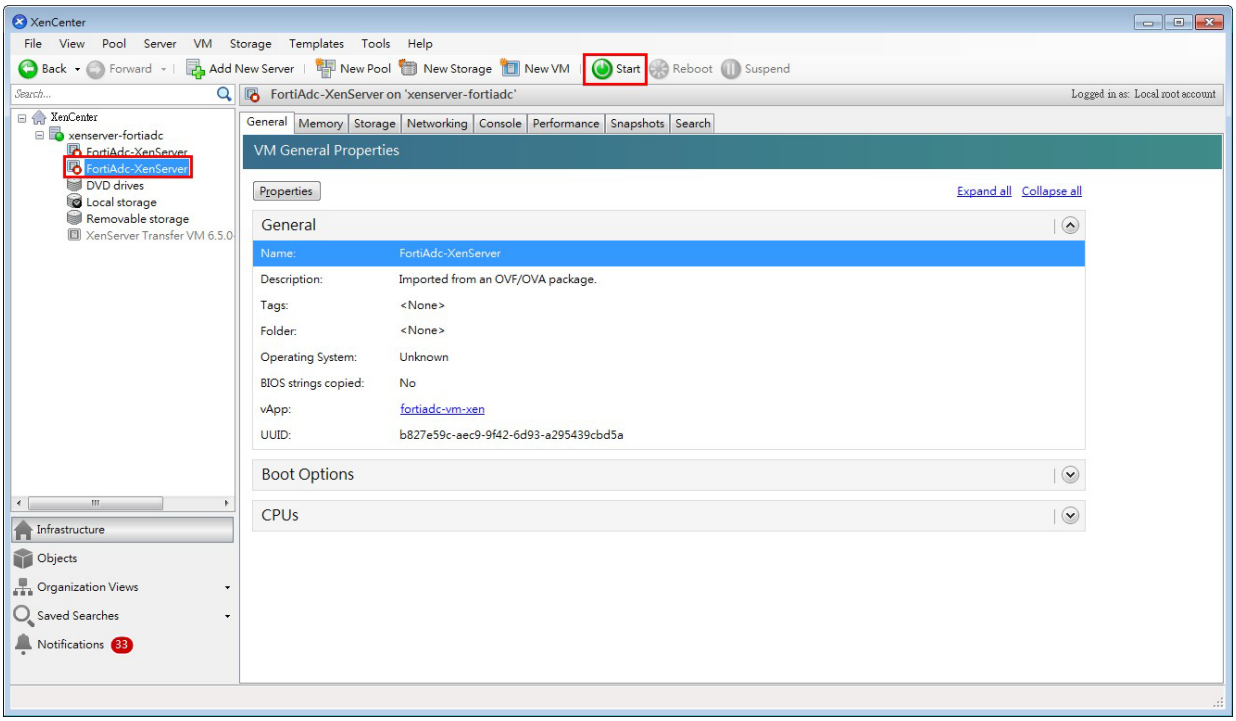
Before you begin:

- You must have mapped the virtual network adapters.
- You must have resized the disk (VMDK), CPUs, and RAM, if necessary.

These settings must be configured in virtual machine environment.

To power on FortiADC-VM:

1. Log into the Citrix XenServer.
2. In the pane on the left side, click the name of the virtual appliance, such as **FortiADC-VM**.
3. Click **Start**.

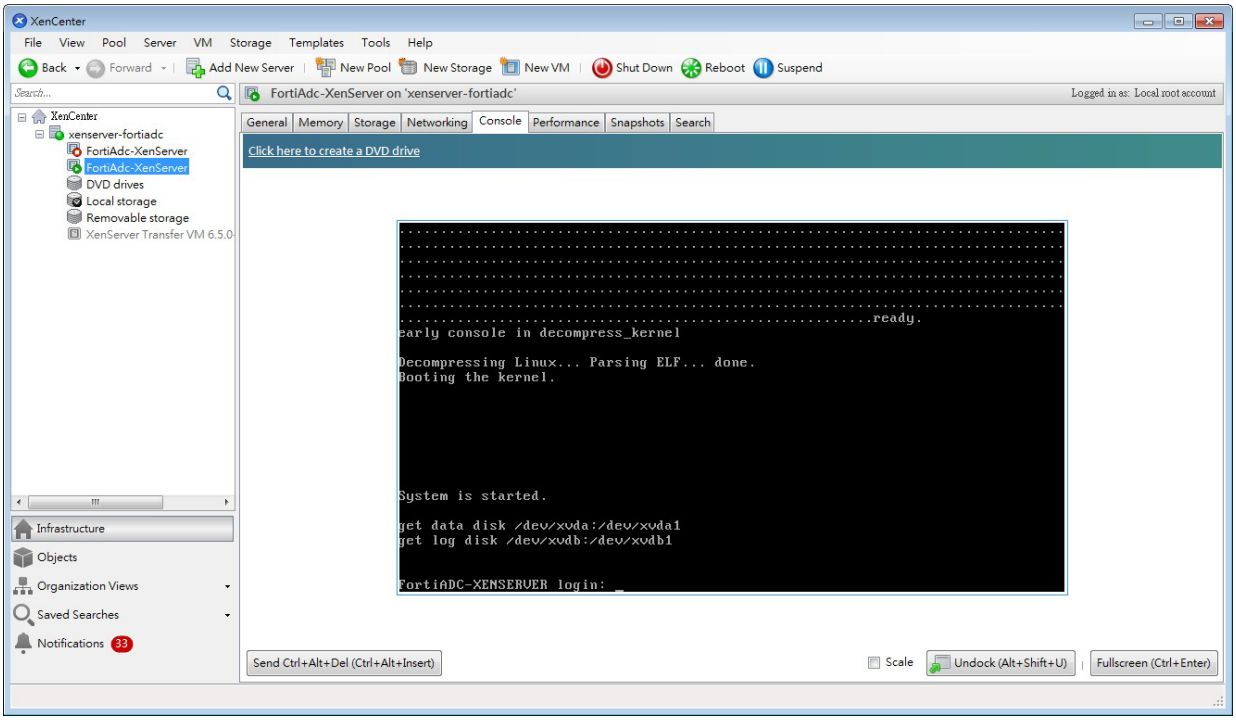


Step 4: Configure access to the web UI & CLI

Once it is powered on, you must log in to the FortiADC-VM command-line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. Log into Citrix XenCenter server.
2. In the left pane, select the name of the virtual appliance.
3. In the right pane, click the **Console** tab to open the console.



4. At the login prompt, type `admin` and no password to log in.
5. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit port1
      set ip <address/mask>
      set allowaccess {http https ping snmp ssh telnet}
end
config router static
   edit 1
      set gateway <gateway_address>
end
config system dns
   set primary <dns_address>
   set secondary <dns_address>
end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.
- `<gateway_address>}` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

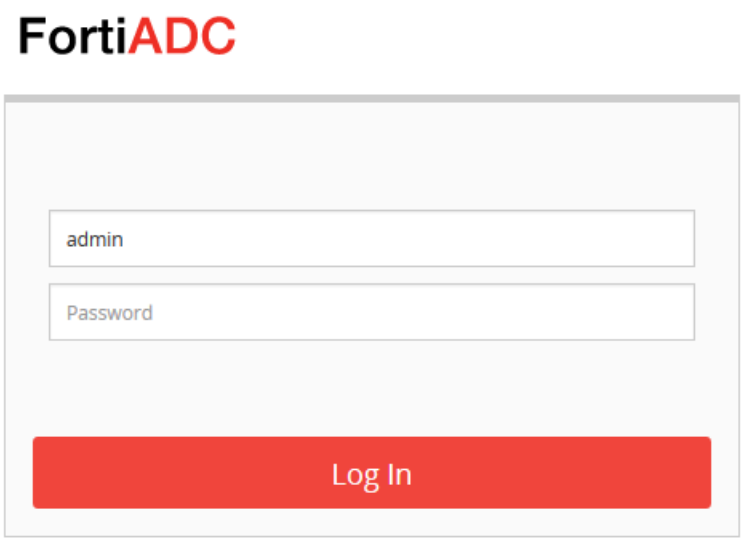
Step 5: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

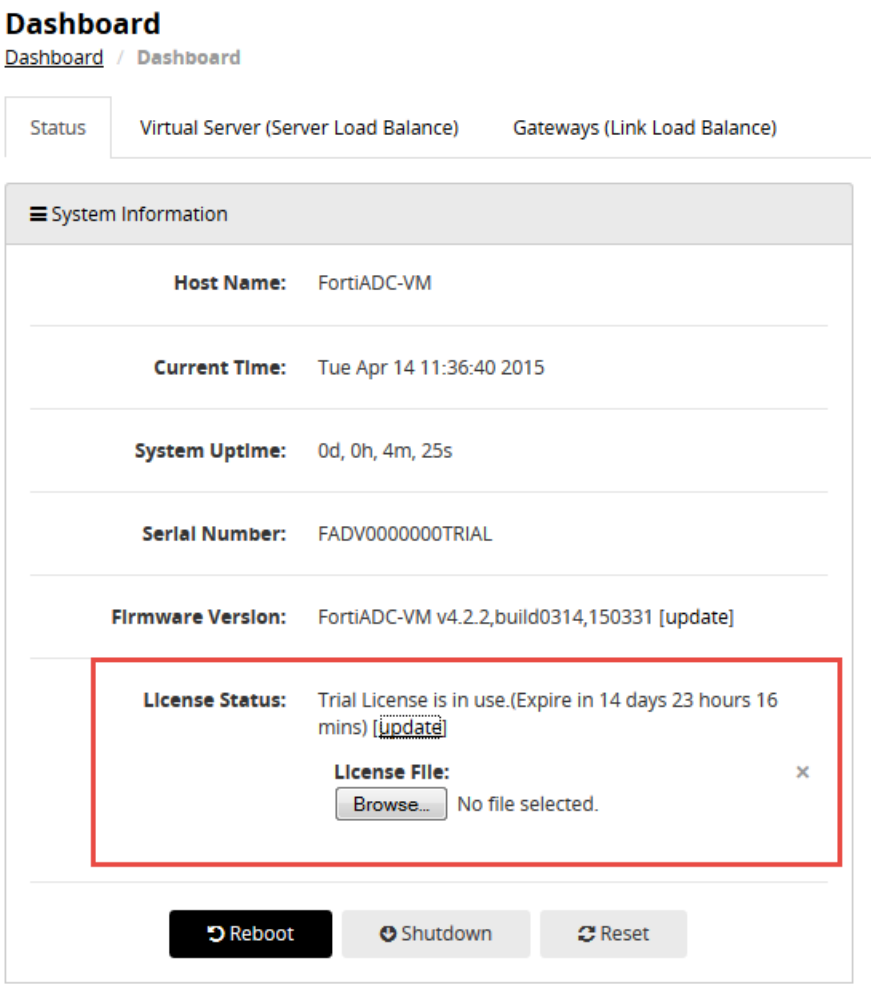
You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as: `https://192.168.1.99/`.
   The web UI login page appears.



3. Use the username `admin` and no password to log in.
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The web UI opens to the dashboard.
5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

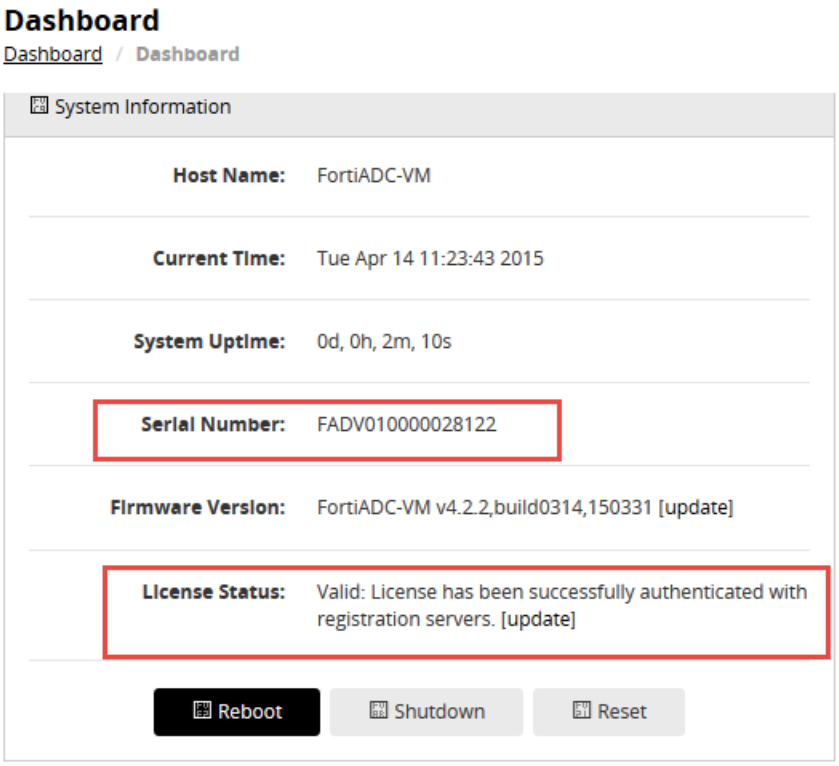


After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```



If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
```

```
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

What's next?

At this point, the FortiADC virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the *FortiADC Handbook* for information on getting started with feature configuration.

Chapter 6: Deploying FortiADC-VM on Xen Project

This chapter provides procedures for FortiADC-VM on Xen Project. It includes the following information:

Installation overview

FortiADC-VM is deployed as a fully virtualized `domU` virtual machine.

To deploy FortiADC-VM on a open source Xen Project hypervisor/XAPI cloud, you can use either the `dom0` virtual machine's:

- command line or
- desktop environment, such as GNOME or KDE

Once FortiADC-VM is deployed, however, either your Xen server itself or your management computer must have a desktop environment.

`sudo xm console <domain_int>` using an alias to `/dev/pty` does not succeed. Instead, VNC is required to connect to FortiADC-VM's virtual local console.

Step 1: Bridge to one of the Xen server physical network interfaces

If you have not yet installed the network bridge utilities required by Xen in order to bridge the virtual machine vNICs to the hypervisor network connection, you must do that by installing the bridge network utilities and then editing the network interface configuration.

```
sudo apt-get install bridge-utils
sudo nano /etc/network/interfaces
```

When editing the network interface configuration, usually you should bind the bridge (in the `vif` examples, the bridge is `xenbr0`) to one of your network interfaces (e.g. `eth0`) in `/etc/network/interfaces`. Depending on the number of physical interfaces on the server and how you will map them to vNetworks, you may need to create multiple bridges.

The following table provides an example of how vNICs could be mapped to the physical network ports on a server with two physical NICs.

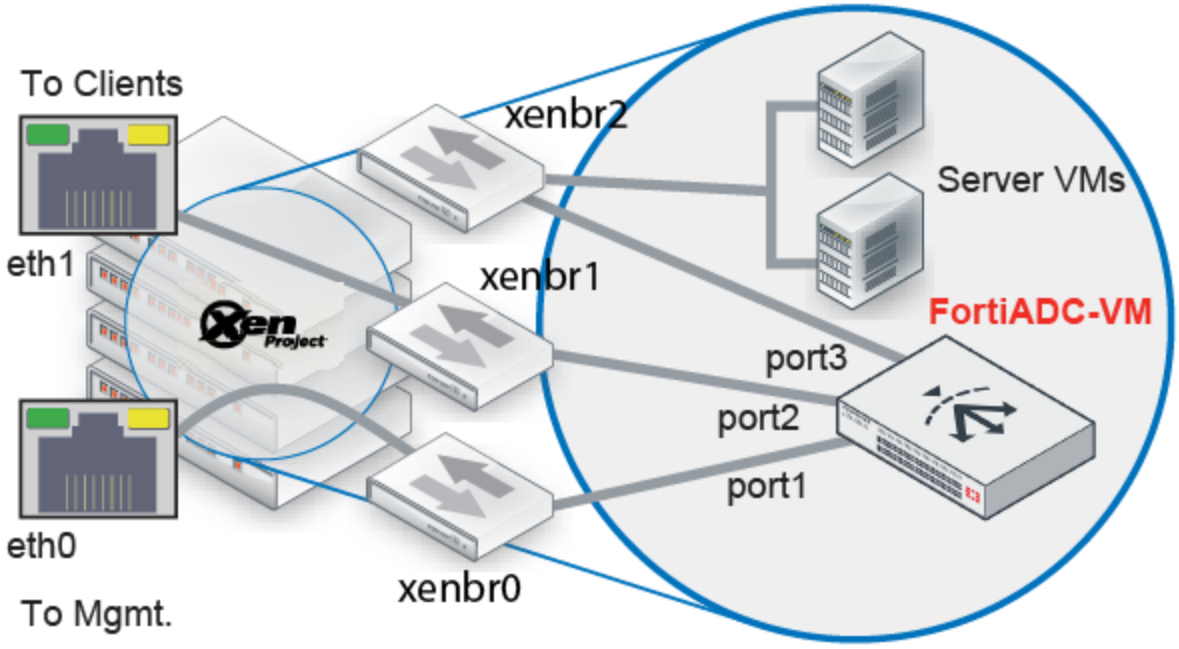


Table 7: Example: Network mapping for reverse proxy mode

Xen Project			FortiADC-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiADC-VM**	**Network Interface Name in Web UI/CLI**
eth0	xenbr0	Management	port1
eth1	xenbr1	External	port2
	xenbr2	Internal	port3

Below is a configuration example assuming the server has only one physical NIC, `eth0`:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto xenbr0
iface xenbr0 inet static
address 192.0.2.10
netmask 255.255.255.0
gateway 192.0.2.1
```

Step 2: Create the VM instance logical volume

You must create the logical volume that FortiADC-VM will use to store its vDisks. In this case, the logical volume is on the Xen server's local disk, but usually it is preferable to store it on an NFS or CIFS share.

To create a local logical volume:

1. Connect to the command line in `dom0` on the Xen server where you will deploy FortiADC-VM (for example, via an SSH client such as PuTTY).
2. Find the name of your `dom0` logical volume group. (Volume group is highlighted below in bold).

```
xenuser@LabXen:~$ sudo pvs
[sudo] password for xenuser:
PV VG Fmt Attr PSize PFree
/dev/sda5 LabXen-vg lvm2 a- 698.39g 673.45g
```

3. Create a logical volume. In this case, the logical volume is on the Xen server's local disk, but you could store it on an NFS or CIFS share.

```
sudo lvcreate -L 100G -n fortiadc-vm /dev/LabXen-vg
```

where you would replace:

- `100G` — The amount of disk space to allocate to FortiADC-VM's vDisk in gigabytes.
- `fortiadc-vm` — The name of your virtual machine, as it appears in Virtual Machine Manager or when you use the `xm` command to create the virtual machine.
- `LabXen-vg` — The name of your `dom0` volume group according to the output of the `sudo pvs` command.

Step 3: Deploy the VM image file

This section describes two options for deploying the VM image file:

- Deploying via Virtual Machine Manager
- Deploying via dom0 command line

Deploying via Virtual Machine Manager

If you have not yet installed a graphical centralized management tool for Xen on your management computer, begin by installing it. Multiple clients exist for managing Xen Project servers. In these instructions, we use Virtual Machine Manager.

On Debian-related Linux distributions, to install Virtual Machine Manager, open a terminal and enter:

```
sudo apt-get install virt-manager
```

On Red Hat-related Linux distributions, the command is :

```
sudo yum virt-manager
```

This centralized manager includes a Xen client for connecting to a remote Xen Project hypervisor to deploy FortiADC-VM. It also includes a built-in VNC client that you will need later in order to connect to FortiADC-VM's

local console and configure its network connection. When the download and installation is complete, if you are not already logged into your desktop environment (GNOME, KDE, xfce, etc.), start X Windows and log in.

To enable Virtual Machine Manager to connect to your Xen server, you must also modify the **server's** configuration file (usually `/etc/xen/xend-config.sxp`). Un-comment these lines (remove the hash (`#`) from the beginning) and change '`no`' to '`yes`':

```
(xend-unix-server yes)
(xend-unix-path /var/lib/xend/xend-socket)
```

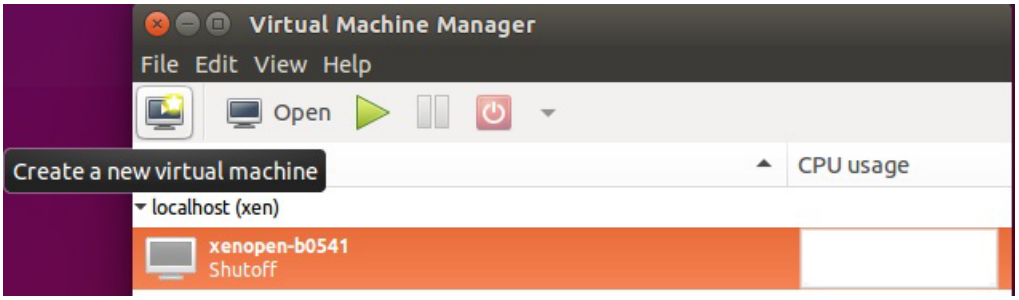
To deploy the VM image using Virtual Machine Manager:

1. On your management computer, open a terminal application and enter the command to extract the package to a folder, then start Virtual Machine Manager:

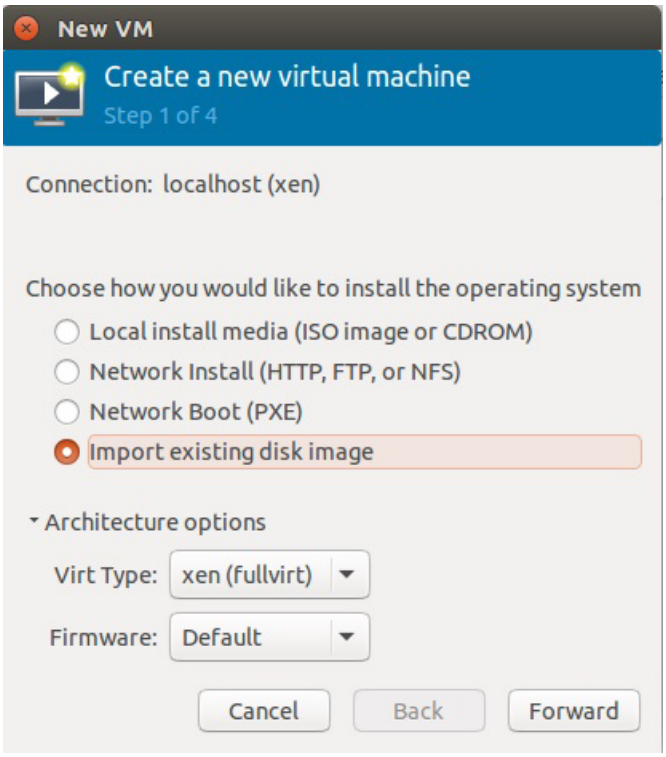
   ```
   unzip FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensource.zip
   sudo virtu-manager
   ```

   The application will open in your desktop environment, so its appearance might vary slightly.

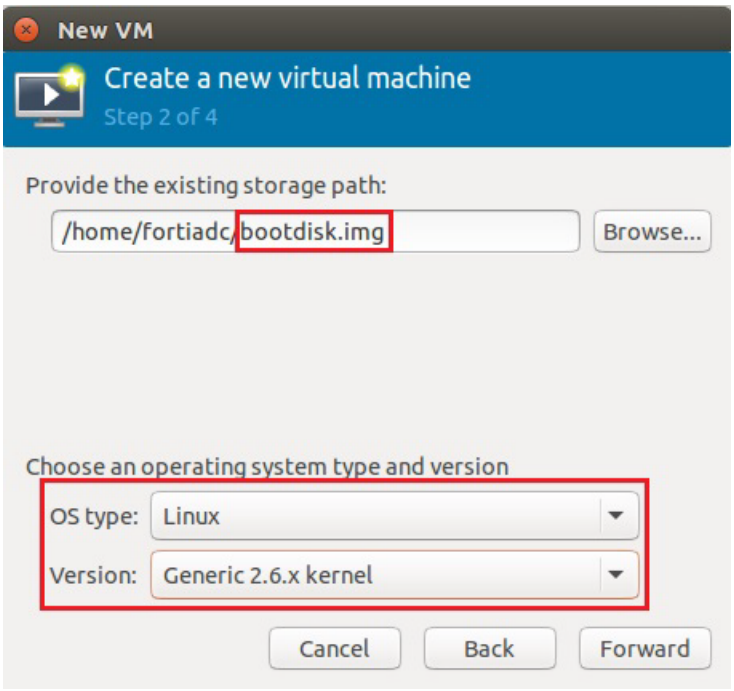
2. Go to File > Add Connection and connect to the Xen server where you will deploy the VM.
3. Click the **New** icon to open the wizard for a new virtual machine.



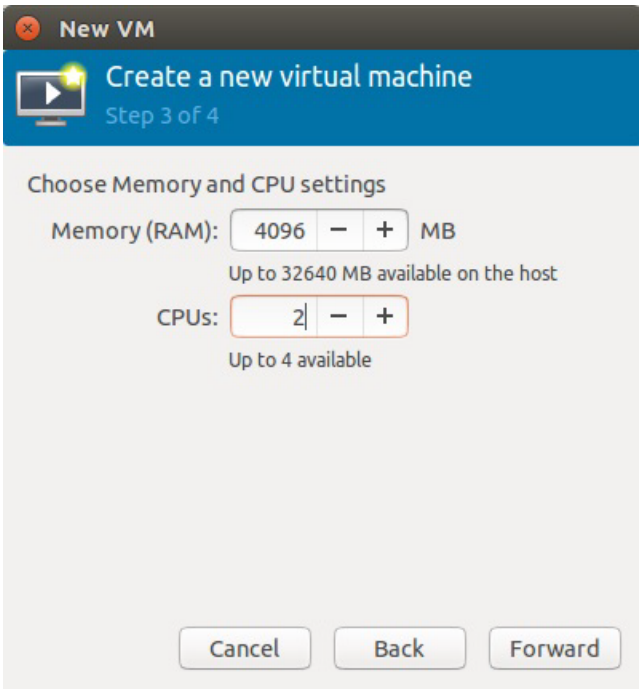
4. Select **Import existing disk image**, select Virt Type **xen (fullvirt)**, and then click **Forward**.



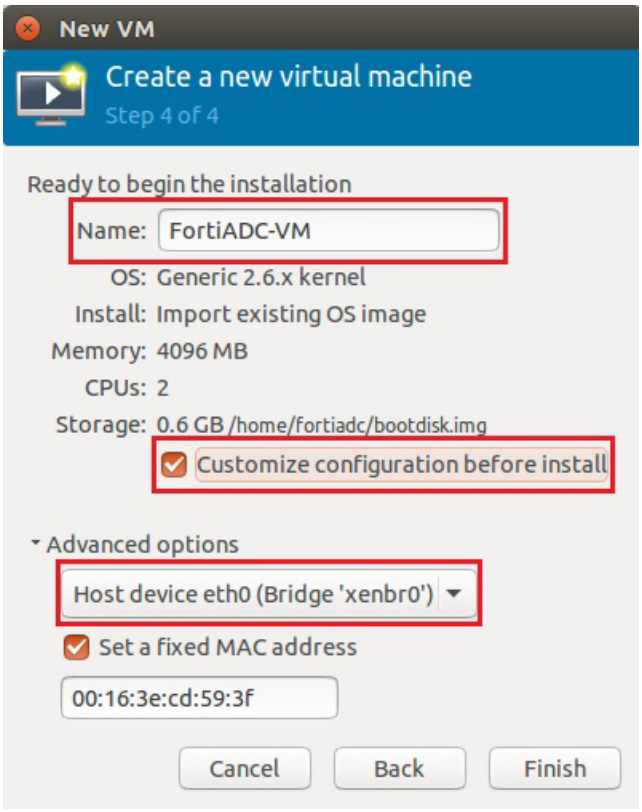
5. Click **Browse** and locate the `bootdisk.img` file. In OS type, select **Linux**, then in Version, expand the list to show all distributions, then select **Generic 2.6.x kernel**, and click **Forward**.



6. Adjust the vRAM and vCPU settings to be appropriate for your deployment. Fortinet recommends a minimum of 2048 MB vRAM and 1 vCPU. Valid vCPU values range from 1 to 8, depending on your FortiADC-VM license. Click **Forward**.

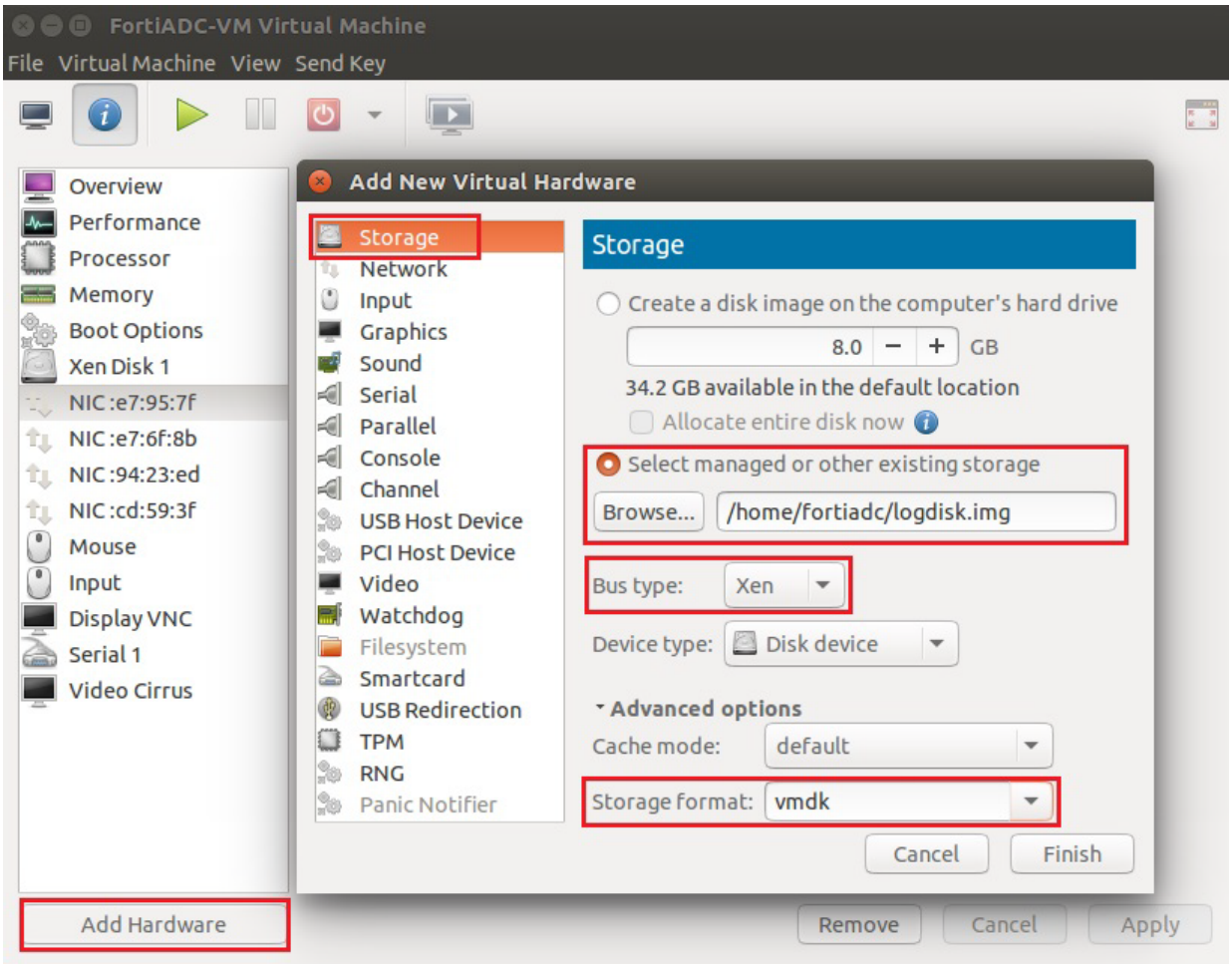


7. In Name, type a unique descriptive name for this instance of FortiADC-VM as it will appear in Virtual Machine Manager's inventory, such as FortiADC-VM. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiADC-VM web UI.) Mark the **Customize configuration before install** check box. Also click to expand **Advanced options**, then click the drop-down menu to change NAT to **Specify shared device name** and in Bridge name, enter the name of the Xen bridge (e.g. `xenbr0`). **Virt Type** should be **xen (fullvirt)**. Click **Finish**.

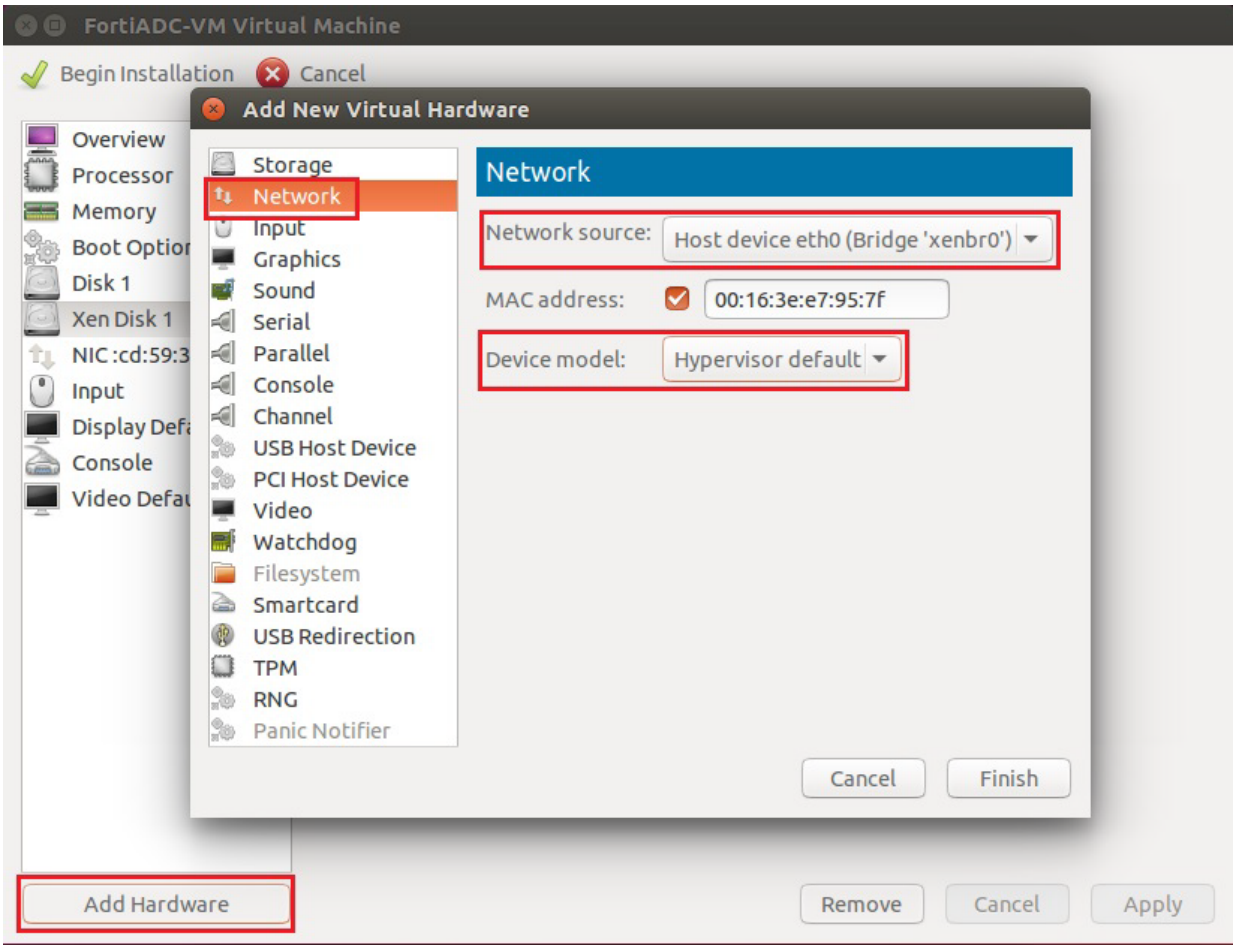


A new dialog will appear where you can add the other vDisk and vNICs.

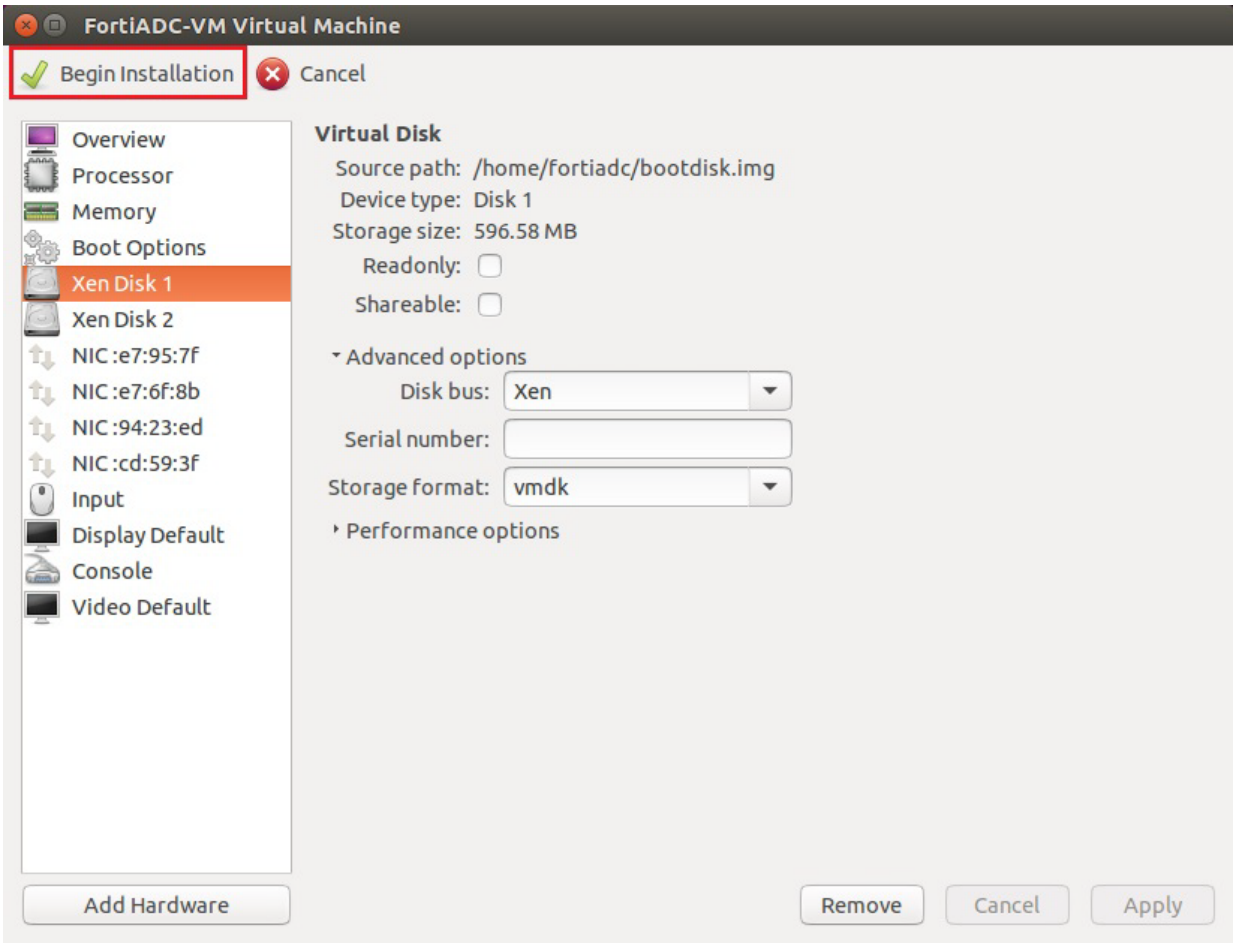
8. In the menu on the left, select the virtual disk. In Advanced options, configure `boot.disk` to be a virtual disk (VMDK). Then click the **Add Hardware** button virtual disk (VMDK). Then click the Add Hardware button and add the logdisk.img file also as a VMDK.



9. In the menu on the left, click **Add Hardware** and add another virtual network adapter that is bound to the bridge. Repeat this step again until you have 4 vNICs, then click **Apply**.



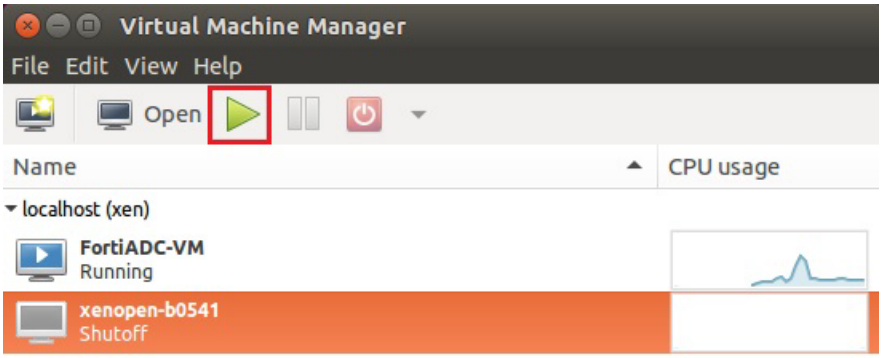
10. Click **Begin Installation** to send the FortiADC-VM image and its VM settings to the Xen server.



The client connects to the VM environment, and deploys the image to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take 15 minutes to complete.

When complete, the deployment should appear in the list of deployed VMs for that Xen server, in the pane on the left side of Virtual Machine Manager.

11. To power on the VM, click the **Play** button.



Deploying via dom0 command line

Connect to the command line of your `dom0` guest. For example, you may be able to use PuTTY to make an SSH connection to the Xen server's IP address, or you may use a local GNOME Terminal application.

Next, unpack the file that you downloaded from Fortinet, and open the configuration file in a plain text editor such as `nano`.

```
unzip FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensource.zip
cd FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensource
nano fortiadc.hvm
```

Then edit these lines in `fortiadc.hvm` file:

```
memory = 4096
vcpus = 2
vif = [ 'type=netfront, bridge=xenbr0', 'type=netfront, bridge=xenbr0', 'type=netfront,
    bridge=xenbr0', 'type=netfront, bridge=xenbr0', ]
disk = [ 'file:<disk image path>/bootdisk.img,xvda,w','file:<logdisk image
    path>/logdisk.img,xvdb,w' ]
```

As an alternative to locally stored disk images, you can reference an NFS or CIFS share:

```
#Mount point on the server's local file system
root = "/dev/nfs"
nfs_server = '192.0.2.100'
#Root directory on the NFS server
nfs_root = '/path/to/directory'
```

Configure virtual hardware settings to allocate appropriate resources for the size of your deployment before powering on the virtual appliance. For details, see the documentation for the open source Xen Hypervisor.

Change the value if necessary to allocate enough vCPUs for the size of your deployment. Valid vCPU values range from 1 to 8, depending on your FortiADC-VM license.

Similarly, FortiADC-VM for Xen Project comes pre-configured to use 4 GB of vRAM (`memory`). However, this is not enough for most deployments. Change this value to be appropriate for your deployment. The valid range is from 2 GB to 16 GB.

If you configure the virtual appliance's storage to be internal (that is, local, on its own vDisk), resize the vDisk before powering on. The FortiADC-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. Resize the vDisk before powering on the virtual machine.

This step is not applicable if the virtual appliance will use external network file system (such as NFS or CIFS) datastores.

Depending on your Xen `dom0` platform, you may also need to reconfigure `fortiadc.hvm` with the path to your `hvmloader`. For example, this may be correct for CentOS or Red Hat Linux:

```
kernel = "/usr/lib/xen/boot/hvmloader
```

but this is required by Ubuntu 12.0.4 LTS:

```
kernel = "/usr/lib/xen-4.1/boot/hvmloader
```

Apply the changes by rebooting or restarting networking. (In some cases rebooting is required: `sudo /etc/init.d/networking restart` may not delete your old IP address from `eth0` and therefore not correctly bring up all interfaces.)

Run these commands to deploy the VM, power it on, and show its Xen domain ID number (highlighted below in bold):

```
xenuser@LabXen:/$ sudo xm create fortiadc.hvm
xenuser@LabXen:/$ sudo xm list
Name ID Mem VCPUs State Time(s)
Domain-0 0 5877 4 r----- 1556.9
fortiadc-vm 2 2048 2 -b---- 126.8
```

If your `dom0` is Ubuntu 12.04 and/or when creating the VM, you receive this error:

```
Error: Domain 'fortiadc-xen' does not exist.
```

and if `/var/log/xen/qemu-dm-fortiadc-xen.log` contains this line:

```
Could not read keymap file: '/usr/share/qemu/keymaps/en-us'
```

then the key mapping is not in its expected location. Enter this line:

```
sudo ln -s /usr/share/qemu-linaro /usr/share/qemu
```

then retry the command to create FortiADC-VM.

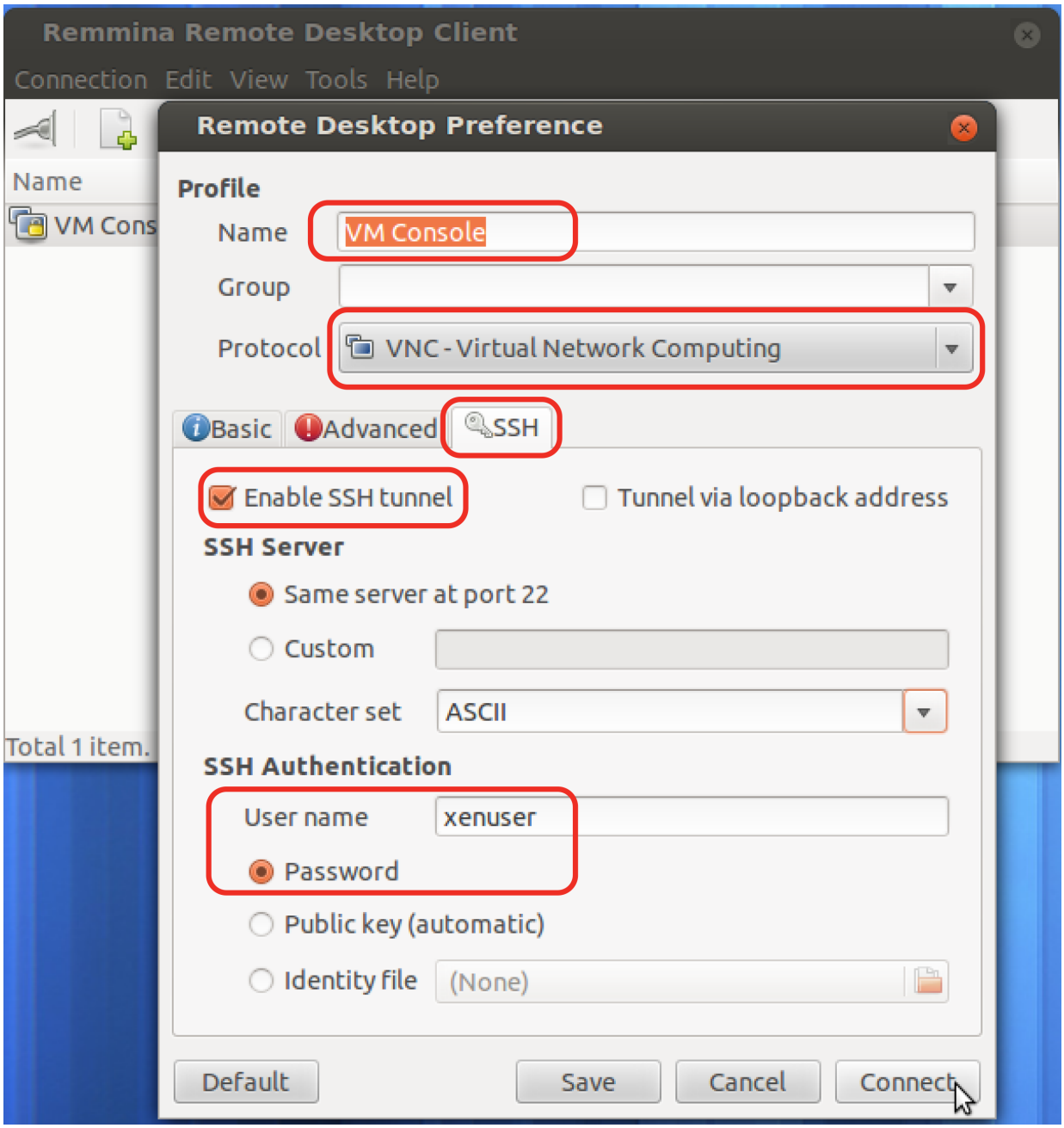
Since VNC listening port numbers are dynamically allocated to guest VMs, use the domain ID number in the output from the previous command to run this command to show the current VNC listening port number and IP address for FortiADC-VM:

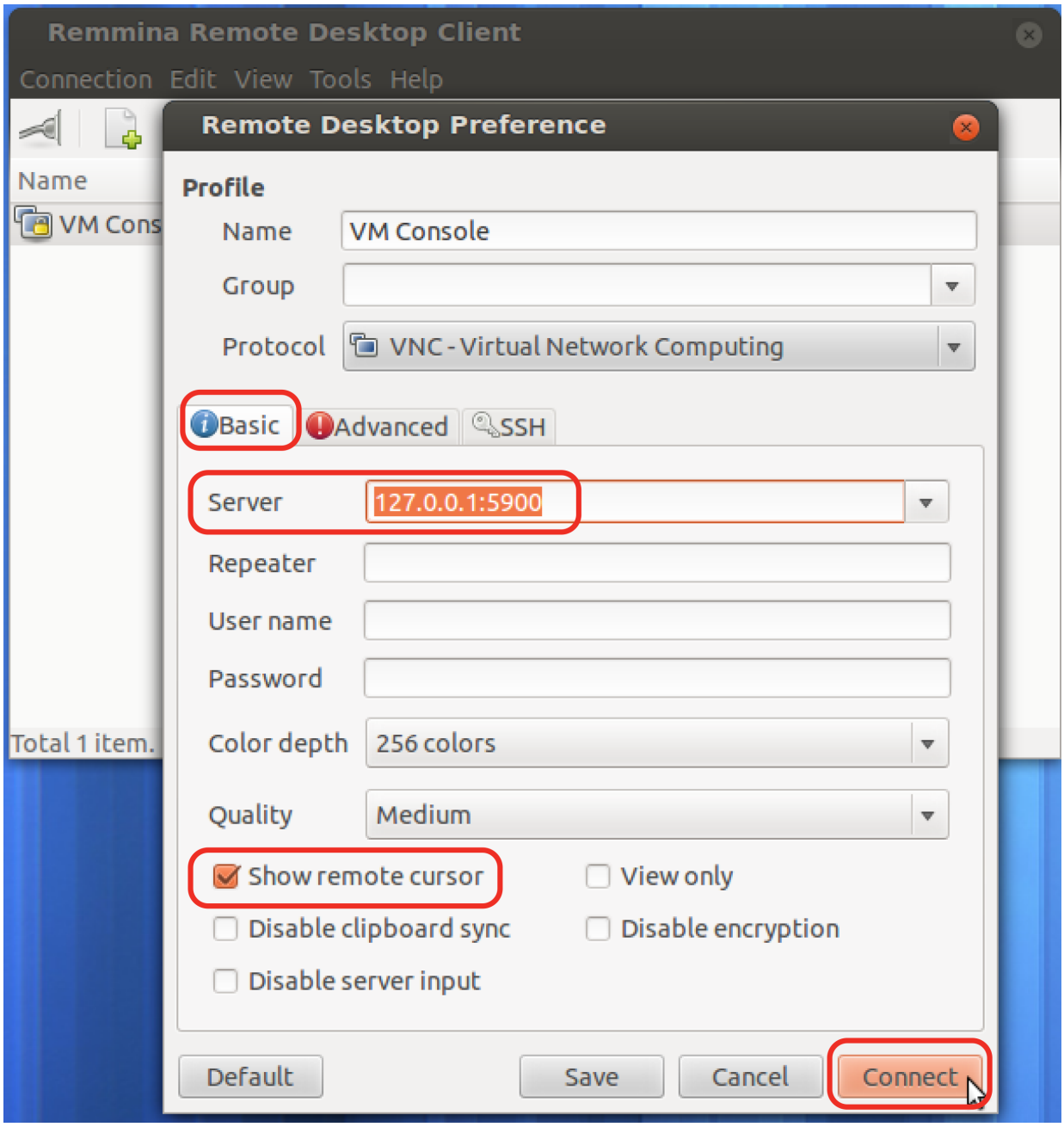
```
xenuser@LabXen:/$ sudo xenstore-ls /local/domain/2/console
port = "4"
limit = "1048576"
type = "ioemu"
vnc-port = "5900"
vnc-listen = "127.0.0.1"
tty = "/dev/pts/5"
```

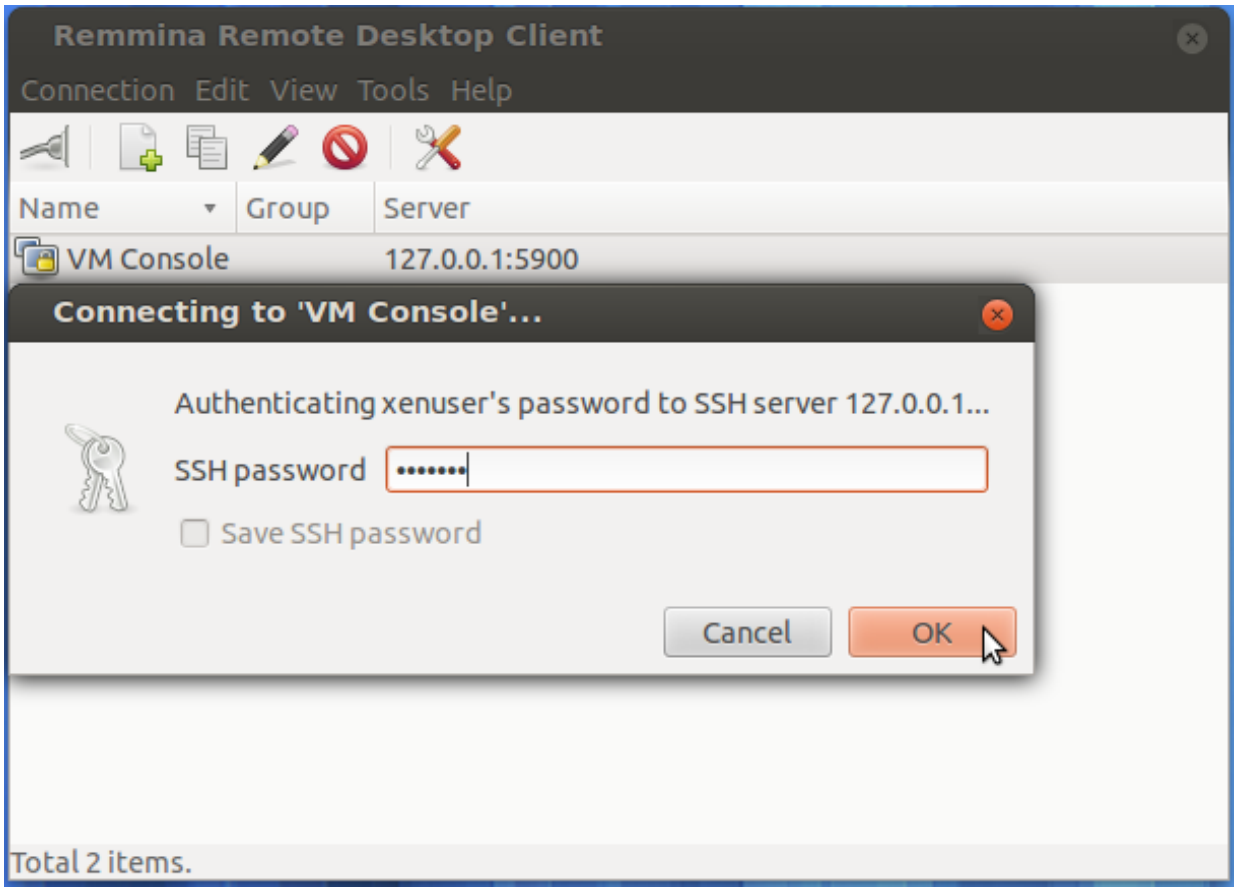
Finally, on your management computer, install and start a VNC viewer and connect to the Xen server's IP address and listening port number for VNC. (In the images below, the VNC viewer is installed in `dom0` on the Xen server that is hosting FortiADC-VM, so the VNC viewer connects to 127.0.0.1. If connecting from your management computer, replace this with the IP address of your Xen server.) For example, on a Debian or Ubuntu Linux management computer, you could use these commands:

```
sudo apt-get install remmina
remmina
```

You **must** run this command from a terminal with an X Windows environment such as GNOME Terminal in order for it to be able to open the VNC viewer window.


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference
Profile
Name
VM Console
Group
Protocol
VNC - Virtual Network Computing
Basic
Advanced
SSH
Enable SSH tunnel
Tunnel via loopback address
SSH Server
Same server at port 22
Custom
Character set
ASCII
SSH Authentication
User name
xenuser
Password
Public key (automatic)
Identity file
(None)
Default
Save
Cancel
Connect


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference
Profile
Name
VM Console
Group
Protocol
VNC - Virtual Network Computing
Basic
Advanced
SSH
Server
127.0.0.1:5900
Repeater
User name
Password
Color depth
256 colors
Quality
Medium
Show remote cursor
View only
Disable clipboard sync
Disable encryption
Disable server input
Default
Save
Cancel
Connect



Step 4: Configure access to the web UI & CLI

Once it is powered on, you must log in to the FortiADC-VM command-line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings in FortiADC-VM:

1. Open the Xen Project Virtual Manager.
2. In the left pane, select the name of the virtual appliance and click **Open**.
3. At the login prompt, type `admin` and no password to log in.
4. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
   edit port1
      set ip <address/mask>
      set allowaccess {http https ping snmp ssh telnet}
end
config router static
   edit 1
      set gateway <gateway_address>
end
```

```
config system dns
   set primary <dns_address>
   set secondary <dns_address>
end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.
- `<gateway_address>}` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

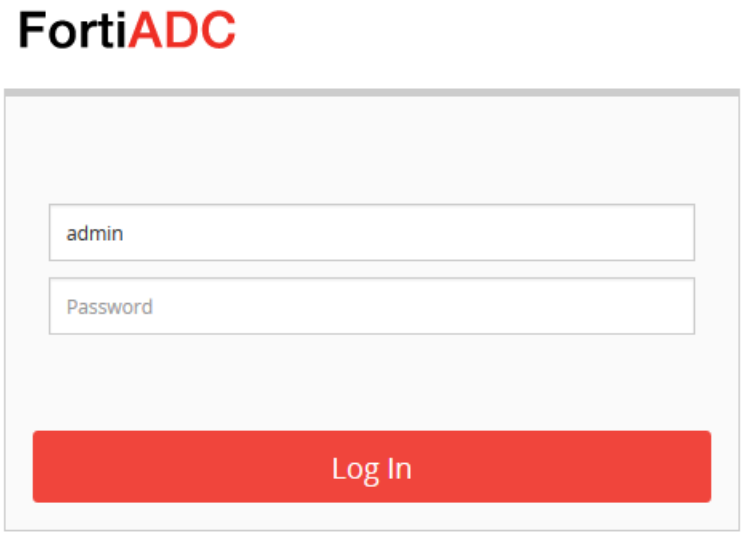
Step 5: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

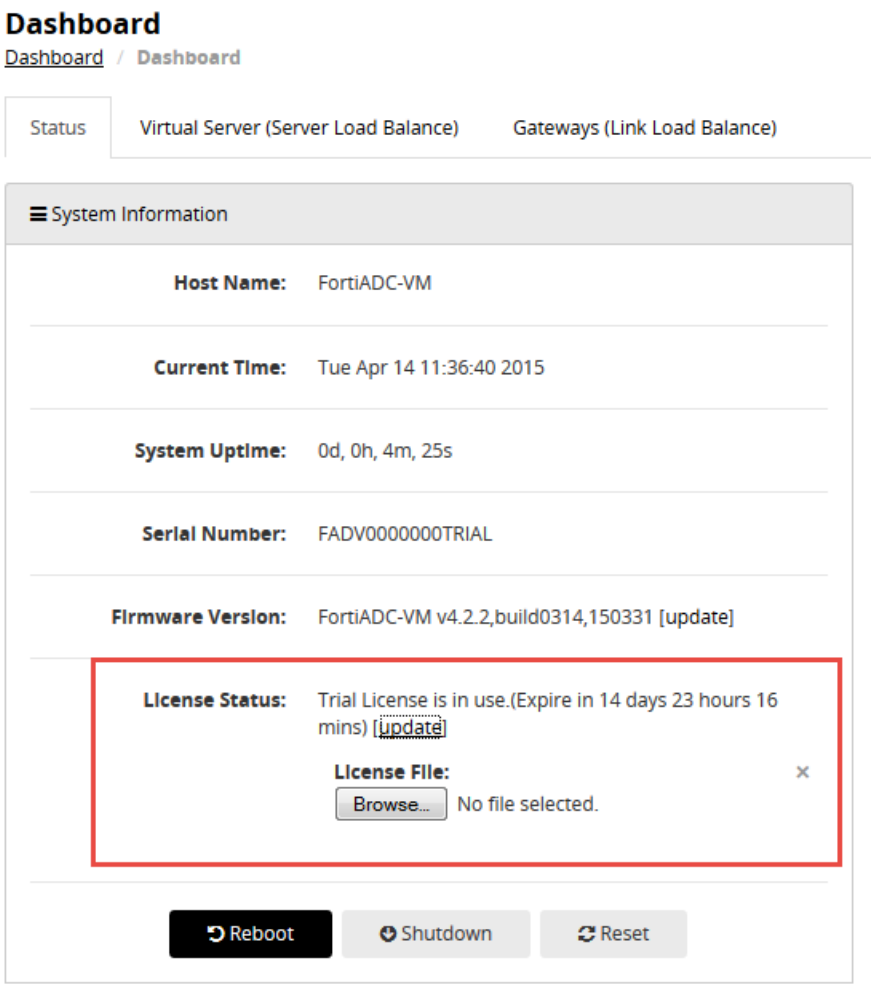
You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
   Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as: `https://192.168.1.99/`.
   The web UI login page appears.



3. Use the username `admin` and no password to log in.
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The web UI opens to the dashboard.
5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

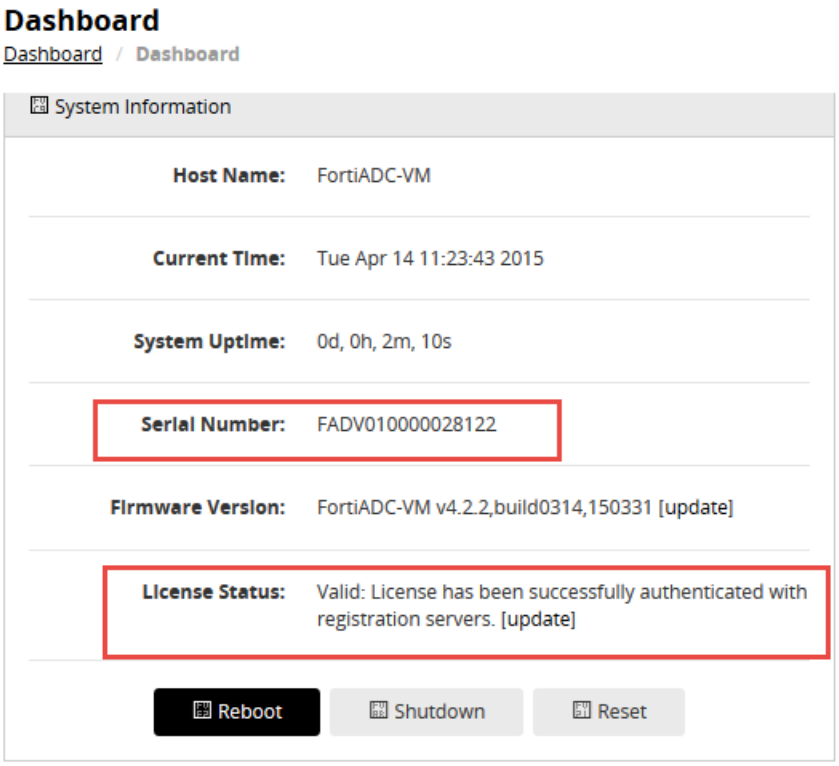


After the license has been validated, the System Information widget indicates the following:

- License row: The message: `Valid: License has been successfully authenticated with registration servers.`
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```



If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
```